Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On the Determination of Groups whose Order is a Power of a Prime.

By J. W. A. Young.

1. Cayley[*] has called attention to an important desideratum in the theory of groups, viz. the determination of all groups of given order n,—two groups of the same order being considered identical when the laws of combination of their elements coincide.[†] He had previously, in papers on the theory of groups as depending on the symbolic equation $\vartheta^n = 1$,[‡] determined the groups in the first case of any difficulty, viz. $n = 8$.

Kempe[||] has given all groups of order 1 to 12, and subsequently Cayley,[§] correcting some errors made by Kempe, gave the groups of the same orders, together with a method of graphic representation. So much by way of enumeration from order to order. On the other hand, Netto[¶] gives all groups of order p^2 and pq, p and q both being prime numbers. Finally, Kronecker[**] has completely determined all commutative groups of any finite order.

2. In the following paper, groups whose order is a power of a prime are considered. In the first paragraph the group-theoretic foundations are laid and a method is reached of classifying groups whose order is a power of a prime in distinct "types". In the second paragraph the groups of order p^3 and those

---

[*] Am. J. Math., Vol. I, p. 50.

[†] *i. e.* all holoedrically isomorphic groups are regarded as identical.

[‡] Phil. Mag., Vol. VII, 1854, pp. 40, 408; Vol. XVIII, 1859, p. 34.

[||] Phil. Trans., Vol. CLXXVII, 1886, pp. 37–43.

[§] Am. J. Math., Vol. XI, p. 139.

[¶] Substitutionentheorie, pp. 133–37. Netto's results are, on the face of it, proved only for groups of substitutions, but they hold generally, since every group can be expressed as a group of substitutions. *Vid.* Cayley, Am. J. Math., Vol. I, p. 52; Dyck, Math. Annalen, Vol. XXII, p. 84.

[**] Berl. Monatsberichte, 1870, p. 881. *Cf.* Schering, Gött. Abhandlungen, July 11, 1868, Vol. XIV.

of order p^4 are completely determined, while the third paragraph is devoted to further consideration of the groups of order 2^4. The fourth paragraph consists of the treatment of those general types in which I have succeeded in finding the distinct groups. The division into types, given in the first paragraph, makes it possible to write out the generating relations of any group of order p^κ, and readily to reduce the question of the identity of two groups to that of "equivalence" of two sets of integers. The method is sufficiently explained and illustrated in the types treated in the second and the fourth paragraph.

3. In the composition of the paper, it has been my aim to presuppose no knowledge of the theory of groups on the part of the reader, and throughout the paper (the notes excepted) the terms used have been defined and the theorems used proved, or else reference has been made to at least one work where such definition or proof may be found. The third paragraph assumes some acquaintance with substitution-groups and with Cayley's method of graphic representation of groups.

I take this opportunity to express my obligation and warmest thanks to Dr. Oskar Bolza, who, throughout the entire course of the investigation, very kindly and materially assisted me with suggestions and counsel, as well as to Professor W. E. Story for valuable criticisms.

§1.

4. The objects of consideration are elements $A_1A_2\ldots.$, $B_1B_2\ldots.$, ... having the following defining properties:*

1) *Multiplication, i. e. a mode of composition, is unambiguously defined, and is associative, but not, in general, commutative.*

2) *Division, i. e. a mode of decomposition, is unambiguously defined, viz. by the property that from* $AB = AC$, *as well as from* $BA = CA$, *shall always follow* $B = C$.

3) *Abstraction is made of all properties of the elements in so far as they are not consequences of these just mentioned; i. e., abstraction is made of the content of the*

---

* Kronecker, Berl. Monatsberichte, 1870, p. 882; Weber, Math. Annalen, Vol. XX, p. 302; Frobenius, Crelle's Journal, Vol. C, pp. 179–80; Perott, Am. J. Math., Vol. XI, pp. 99–101; Hölder, Math. Annalen, Vol. XXXIV, p. 29.

symbol. Two elements B and C are identical when $AB = AC$, as well as $BA = CA$, for every element A.

5. In consequence of 1) the terminology of multiplication is employed and the element AB, resulting from the combination of A and B, is called the *product* of the *factors* A and B. (It is not necessary to the purposes of this paper to make a convention as to which element shall be considered multiplier and which multiplicand.) The element $AA = A^2$, resulting from the combination of the element A with itself, is styled the second *power* of A, and, in general, $A.A.A \ldots . (\alpha \text{ times}) = A^\alpha$, the α^{th} *power* of A.

6. A *group* is an aggregate of elements such that every product of two elements of the aggregate is also contained in the aggregate. The *order* of a group is the number of distinct elements it contains. From the assumptions and definitions above it follows easily:*

a.) That in every group of finite order there exists one, and only one, element A_0 such that for every element A of the group $A_0A = AA_0 = A$; A_0 is called the *principal* element of the group and denoted by the symbol 1.

b.) That, if A_i be any element of the group, there always exists in the group one, and only one, element A_i' such that $A_iA_i' = A_i'A_i = A_0 = 1$. A_i' is called the *inverse* of A_i and is written A_i^{-1}.

7. If the group contains the elements $A_1, A_2, \ldots . A_m$, every expression of the form

$$A_1^{\alpha_{11}} A_2^{\alpha_{12}} \ldots . A_m^{\alpha_{1m}} A_1^{\alpha_{21}} A_2^{\alpha_{22}} \ldots . A_m^{\alpha_{2m}} \ldots . A_1^{\alpha_{l1}} A_2^{\alpha_{l2}} \ldots . A_m^{\alpha_{lm}}$$

is also an element of the group. If it happens that *every* element of the group can be expressed in terms of the elements $A_1A_2 \ldots . A_m$ in the form just given, $A_1A_2 \ldots . A_m$ are called a *system of generating elements* of the group. A group is completely defined when the laws of combination of a system of generating elements are given, and is said to be *generated by* these elements. The laws of combination are always expressible as equalities between two products of the form given above, or, denoting such a product by $F(A_1A_2 \ldots . A_m)$ as

$$F_1(A_1A_2 \ldots . A_m) = F_2(A_1A_2 \ldots . A_m).$$

By multiplying by the inverses of the elements on the right, these relations

---

*Kronecker, Weber, *l. c.*

can always be brought into the form $F(A_1 A_2 \ldots\ldots A_m) = 1$, or, for brevity, $F = 1$.

8. From the given relations others usually follow as consequences. In the determination of groups of a given order it is of importance that all the consequences of the relations given be *explicitly* considered. The consequences of given relations are obtained by the following method:*

Let $F = 1$ be a relation between the generating elements $A_1 A_2 \ldots\ldots A_m$. If

$$F = A_1^{\alpha_{11}} A_2^{\alpha_{12}} \ldots\ldots A_m^{\alpha_{1m}} A_1^{\alpha_{21}} A_2^{\alpha_{22}} \ldots\ldots A_m^{\alpha_{2m}} \ldots\ldots A_1^{\alpha_{r1}} A_2^{\alpha_{r2}} \ldots\ldots A_m^{\alpha_{rm}} = 1,$$

it follows, multiplying this equality by itself, that

$$A_1^{\alpha_{11}} \ldots\ldots A_m^{\alpha_{1m}} \ldots\ldots A_1^{\alpha_{r1}} \ldots\ldots A_m^{\alpha_{rm}} . A_1^{\alpha_{11}} \ldots\ldots A_m^{\alpha_{1m}} \ldots\ldots A_1^{\alpha_{r1}} \ldots\ldots A_m^{\alpha_{rm}} = 1,$$

which we may write $F^2 = 1$. So, in general, it follows from the relation $F = 1$, that also $F^\alpha = 1$, for all positive integral values of α. But there may be still other consequences of $F = 1$, viz., if $F = 1$ be transformed† by each of the generating elements there follow the relations

$$A_i^{-1} F A_i = 1. \qquad i = 1, 2 \ldots\ldots m.$$

These relations may all be identical with $F = 1$, (as in the case that the elements $A_1, A_2, \ldots\ldots A_m$ are all commutative with one another). In such a case, the only consequences of the relation $F = 1$ are its own powers. If any of the relations found by transformation are distinct from $F = 1$, they must be transformed again by each of the generating elements, and so on until a system of relations is reached such that when any relation of the system is transformed by any generating element of the group, the resulting relation is already contained in the system. This system, together with all the products and powers of relations contained in it, is a complete system of the consequences of the relation $F = 1$. If there exist other relations, $F_2 = 1$, $F_3 = 1, \ldots\ldots F_l = 1$, they must be treated similarly. All products of relations of the different systems so found are also consequences. But nothing new will be reached by transforming relations like

$$F_1 F_2 = 1,$$

for $A_i^{-1} F_1 F_2 A_i = A_i^{-1} F_1 A_i . A_i^{-1} F_2 A_i$, and this is a product of a consequence of F_1 and a consequence of F_2.

---

* Dyck, Math. Annalen, Vol. XX, p. 12.

† An element B is said to be "transformed" by A when the product $A^{-1}BA$ is formed, and the element $A^{-1}BA$ is called "the transformed" of B by A.

If, therefore, a group be generated by a system of elements $A_1 A_2 \dots . A_m$, satisfying the relations $F_1 = 1$, $F_2 = 1, \dots . F_l = 1$, a complete system of the relations consequent upon these is obtained by transforming each relation, as well as all the new relations so resulting, by all the generating elements of the group; adding all the new relations so found to the original system; and finally, when nothing new arises by transformation, including all the different products and powers of the relations hitherto known.

9. A system of generating elements may always be found containing any given element of the group, but if the group contains an element different from unity, there will be systems of generating elements that do not contain *all* the elements of the group. The same group may therefore be variously defined by different choices of the generating elements and consequent variation in the relations between them.

To find all distinct groups of a given order we consider first all possible systems of relations between elements which will generate a group of the given order; and secondly, determine which of the groups so generated are distinct. That two groups of order N, defined by two systems of relations, may be identical, it is necessary and sufficient that each group contain elements which satisfy all the generating relations of the other group, but no relation independent of these. For under these conditions each group is contained in the other, i. e. the groups are identical.*

10. *Groups of order p^κ; p a prime.*

Sylow† has proved the following theorem:

If the order of a group is p^κ, p being a prime, any element A of the group is represented once and only once by the expression

$$A = A_0^i A_1^j A_2^l \dots . A_{\kappa-1}^m,$$

when $i, j, l, \dots . m = 0, 1 \dots . p-1$, independently, and where $A_0, A_1, \dots, A_{\kappa-1}$ are elements of the group satisfying the following relations:

$$\begin{aligned} A_0^p &= 1 \\ A_1^p &= A_0^a \\ A_2^p &= A_0^b A_1^c \\ &\dots\dots\dots\dots\dots\dots \\ A_{\kappa-1}^p &= A_0^r A_1^s \dots . A_{\kappa-2}^t, \end{aligned}$$

---

* Poincaré, Acta Math., Vol. I, p. 10.

† Math. Annalen, Vol. V, p. 588.

and also (A being any element of the group)

$$
\begin{aligned}
A^{-1}A_0A &= A_0\\
A^{-1}A_1A &= A_0^{\alpha}A_1\\
A^{-1}A_2A &= A_0^{\beta}A_1^{\gamma}A_2\\
&\cdots\cdots\cdots\cdots\cdots\\
A^{-1}A_{\kappa-1}A &= A_0^{\pi}A_1^{\rho}A_2^{\sigma}\cdots\cdots A_{\kappa-2}^{\omega}A_{\kappa-1}.
\end{aligned}
$$

The exponents $a, b, c \dots\dots t, \alpha, \beta, \gamma, \dots\dots \omega$, *may take independently the values* $0, 1, \dots\dots p-1$.

This theorem assures that, when the exponents take successively all possible sets of values, all groups of the order are represented at least once, but it remains to determine which of the groups so represented are distinct; or, in other words, given two sets of exponents in Sylow's formulæ, to decide whether or not the corresponding groups are identical. Instead, however, of thus starting from Sylow's theorem, it is more convenient to introduce a modified classification which makes, from the very beginning, a considerable restriction in the number of possibilities to be considered. This classification is based upon the following theorem, which is the foundation of Sylow's theorem just cited, and is proved by him in that connection:

Every group whose order is a power of a prime contains at least one element which is different from unity and commutative with every element of the group.

11. It follows immediately from this theorem* that every group G, of order p^{κ}, contains a subgroup $\Gamma^{(1)}$, of order p^{κ_1}, $\kappa_1 > 0$, consisting of the totality of all the elements of G which are commutative with every element of G. The two groups G and $\Gamma^{(1)}$ suffice to define, as follows, a new group, called the *quotient* of G by $\Gamma^{(1)}$.†

The elements of G can be arranged in the following table, in which the subgroup $\Gamma^{(1)}$ constitutes the first row:

$$
\begin{array}{llll}
1, & A_2, & A_3 & \dots\dots A_{p^{\kappa_1}}\\
B_2, & A_2B_2, & A_3B_2 & \dots\dots A_{p^{\kappa_1}}B_2\\
\cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\
B_{p^{\kappa-\kappa_1}}, & A_2B_{p^{\kappa-\kappa_1}}, & A_3B_{p^{\kappa-\kappa_1}} & \dots\dots A_{p^{\kappa_1}}B_{p^{\kappa-\kappa_1}}.
\end{array}
$$

We form the product of any two elements of the table:

$$A_{\alpha}B_{\beta}A_{\alpha'}B_{\beta'} = A_{\alpha}A_{\alpha'}B_{\beta}B_{\beta'} = A_{\alpha''}B_{\beta}B_{\beta'}.$$

---

* Netto, Substitutionentheorie, p. 49.

† Hölder, Math. Annalen, Vol. XXXIV, pp. 31-33.

The *row* of $A_{\alpha''}B_\beta B_{\beta'}$ is independent of $A_{\alpha''}$, which occurs in every row, and is definitely determined by B_β and $B_{\beta'}$; i. e. from any two rows of the table, taken in a given order, there follows definitely a third. The rows of the table may therefore be considered as elements; they form a group $G^{(1)}$ of order $p^{\kappa-\kappa_1}$. Hölder calls the group $G^{(1)}$, thus determined by G and $\Gamma^{(1)}$, the *quotient* of G by $\Gamma^{(1)}$, and denotes the relation by the equation

$$G^{(1)} = G \,|\, \Gamma^{(1)}.^*$$

Analogously,† $G^{(1)}$ and $\Gamma^{(1)}$ are called the factors of G.

12. Since the group $G^{(1)}$ is independent of the A's, its laws of combination are those of the B's when the factors in the A's are disregarded. The laws of combination of the elements of $G^{(1)}$ are thus unambiguously deduced from the laws of G, by placing therein all the A's equal to unity. To pass conversely from the laws of combination of $G^{(1)}$ to those of G, a factor in the A's must be introduced, and the process is not unambiguous.

13. To the group $G^{(1)}$, of order $p^{\kappa-\kappa_1}$, the previous reasoning can be applied, and thus by successive steps we pass unambiguously from one quotient group to another, until finally a group $G^{(\mu)} = 1$ is reached.

In this process the following groups have been defined:

	ORDER.		ORDER.
G	p^{κ}		
$\Gamma^{(1)}$	p^{κ_1}	$G^{(1)} = G \vert \Gamma^{(1)}$	$p^{\kappa-\kappa_1}$
$\Gamma^{(2)}$	p^{κ_2}	$G^{(2)} = G^{(1)} \vert \Gamma^{(2)}$	$p^{\kappa-\kappa_1-\kappa_2}$
....	....	....	....
....	....	....	....
$\Gamma^{(\mu-1)}$	$p^{\kappa_{\mu-1}}$	$G^{(\mu-1)} = G^{(\mu-2)} \vert \Gamma^{(\mu-1)}$	$p^{\kappa-\kappa_1-\kappa_2-\cdots-\kappa_{\mu-1}}$
$\Gamma^{(\mu)}$	p^{κ_μ}	$G^{(\mu)} = G^{(\mu-1)} \vert \Gamma^{(\mu)} = 1$	$p^{\kappa-\sum_{i=1}^{\mu}\kappa} = 1$

If two groups, G_1 and G_2, are identical, their subgroups $\Gamma_1^{(1)}$ and $\Gamma_2^{(1)}$, unambiguously defined as above, must be identical, and the quotient groups $G_1^{(1)}$ and $G_2^{(1)}$ must also be identical. The converse does not necessarily hold.

---

* *Any* self-conjugate subgroup is sufficient for the determination of a quotient group. The group $G^{(1)}$ is meriedrically isomorphic with G.

† Hölder, Math. Annalen, Vol. XXXIV, p. 32; Dyck, Math. Annalen, Vol. XX, p. 14.

Applying the same reasoning to $G^{(1)}$, $G^{(2)} \dots .$, we find that a necessary, though not sufficient, condition for the identity of G_1 and G_2 is that the groups $\Gamma_1^{(i)}$ and $\Gamma_2^{(i)}$, $i = 1, 2 \dots . \mu$, coincide respectively throughout.*

14. The groups $\Gamma^{(i)}$ are all commutative groups;† to them we apply the following theorem:‡

If the elements of a group of order n are all commutative with one another, there can always be found in the group a system of elements $a_1, a_2, \dots . a_m$, *satisfying the relations*

$$a_1^{r_1} = 1,\ a_2^{r_2} = 1,\ \dots .\ a_m^{r} = 1,\ r_1 r_2 \dots . r_m = n,$$

r_i *divisible by* r_{i+1}, *such that the expression*

$$a_1^{h_1} a_2^{h_2} \dots . a_m^{h_m}$$

represents each element of the group once, and only once, when $h_i = 1, 2, \dots . r_i$, *independently*, $(i = 1, 2, \dots m)$.

Every set of r's satisfying the above conditions gives rise to a commutative group of order n, when used as exponents in the above relations. All groups are distinct in which the r's do not coincide throughout.

15. By the theorem just cited, the group $\Gamma^{(i)}$, of order p^{κ_i}, is generated by elements satisfying the relations

$$\begin{aligned} &a_1^{p^{\kappa_{i1}}} = 1,\ a_2^{p^{\kappa_{i2}}} = 1,\ \dots .\ a_{l_i}^{p^{\kappa_{il_i}}} = 1, \\ &a_h a_j = a_j a_h, \quad h, j = 1, 2 \dots . l_i \text{ independently}, \\ &\kappa_{i1} + \kappa_{i2} + \dots . + \kappa_{il_i} = \kappa_i . \end{aligned}$$

The group $\Gamma^{(i)}$ is completely defined by the numbers $\kappa_{i1}, \kappa_{i2} \dots . \kappa_{il_i}$ and the fact that it is a commutative group.

Since G_1 and G_2 cannot be identical unless the groups $\Gamma_1^{(i)}$ and $\Gamma_2^{(i)}$ coincide, the numbers κ_{ij} must coincide respectively throughout, if the groups are identical. This agreement in the values of the numbers κ_{ij} is a necessary, though not sufficient, condition for the identity of two groups. It affords thus a basis of classification. We shall say that all the groups leading to the same set of values $\varkappa_{ij}$ constitute a *type*, and denote the type by the symbol

---

* Cf. Hölder, Math. Annalen, Vol. XXXIV, pp. 32-38.

† For brevity we say "commutative groups," instead of "groups whose elements are all commutative with one another."

‡ Kronecker, Berl. Monatsberichte, 1870, p. 881; Schering, Gött. Abhandlungen, 1868, Vol. XIII; Netto, Substitutionentheorie, pp. 144-47; Weber, Math. Annalen, Vol. XX, pp. 304-7; Frobenius u. Stickelberger, Crelle's Journal, Vol. LXXXVI, pp. 224-36. See also Perott, Am. J. Math., Vol. XI, pp. 99-138; Vol. XIII, p. 235.

$$(\varkappa_{11}\varkappa_{12}\dots\varkappa_{1l_1})(\varkappa_{21}\varkappa_{22}\dots\varkappa_{2l_2})\dots(\varkappa_{j1}\varkappa_{j2}\dots\varkappa_{jl_j}).$$

A type is of as many *steps* as there are parentheses in its symbol. The commutative groups are groups of one step. Since groups belonging to different types cannot be identical, it remains to determine all the different groups contained in each possible type.

16. A group which can be generated by a single element is called a *cyclic* group.

In a group of more than one step, the last group $\Gamma^{(\mu)}$ *cannot be a cyclic group.* For convenience, we consider a group of only two steps (such a group must always occur, viz. $G^{(\mu-2)}$) and use the notation of No. 13. To say that $\Gamma^{(2)} = G^{(1)}$ is a cyclic group, is to say that, considering the rows of the table in No. 10 as elements, any element can be expressed as a power of one properly chosen, and that hence the elements B, on which alone the group $G^{(1)}$ depends, must also be powers of one of them.

The group G is then generated by $\Gamma^{(1)}$ and a single element B satisfying the relation $B^{p^{\kappa-\kappa_1}} = A^m$, ($A$ being some element of $\Gamma^{(1)}$). Since all the elements of $\Gamma^{(1)}$ are commutative with every element of the whole group, and there is only one generating element other than those of $\Gamma^{(1)}$, it follows that the group G is commutative, contrary to the hypothesis that it is of two steps. It is, therefore, not possible that the last group $\Gamma^{(\mu)}$ be a cyclic group. In other words, *in a group of more than one step, the last parenthesis of the type symbol must contain more than one integer.*

§2.

17. *Groups of order* p^2.

The formally possible types are

$$(11)$$
$$(2)$$
$$(1)(1)$$

Of these the first two are commutative groups, and the last type is non-existent, according to the result of No. 16.

Permanent notation. All elements of G which are commutative with every element of G, shall be denoted by the letter a (with the necessary indices) and its products and powers, and the letter a shall be restricted to such elements.

18. *Groups of order* p^3.

Types:

$$\left.\begin{array}{l}(111)\\(21)\\(3)\end{array}\right\}\text{commutative groups.}$$

$$(1)(11).$$

Type (1)(11).

The type symbol means that $\Gamma^{(1)}$ is generated by an element a satisfying the relation

$$a^p = 1,$$

and that $G^{(1)} = \Gamma^{(2)}$ is generated by elements $a_1^{(1)}$, $a_2^{(1)}$ satisfying the relations

$$\begin{aligned} a_1^{(1)} &= 1 \\ a_2^{(1)^p} &= 1 \\ a_1^{(1)} a_2^{(1)} &= a_2^{(1)} a_1^{(1)}. \end{aligned}$$

The table of G is (cf. No. 11)

$$\begin{array}{llll|c} & & & & G^{(1)} \\ 1, & a, & a^2, \ldots . a^{p-1}, & & 1 \\ b_2, & ab_2, & a^2 b_2, \ldots . a^{p-1} b_2, & & a_1^{(1)} \\ b_3, & ab_3, & a^2 b_3, \ldots . a^{p-1} b_3, & & a_1^{(1)^2} \\ \ldots & \ldots & \ldots & & \vdots \\ b_{p^2}, & ab_{p^2}, & a^2 b_{p^2}, \ldots . a^{p-1} b_{p^2}. & & a_1^{(1)^{p-1}} . a_2^{(1)^{p-1}} \end{array}$$

Since the elements of $G^{(1)}$ are the rows of G, every element of the row corresponding to $a_1^{(1)^2}$ must be, to within a factor in a, the square of some element in the row corresponding to $a_1^{(1)}$, i. e., with perhaps a change in the order of the elements of the row beginning with b_3, we may write $b_3 = b_2^2$. Similarly it follows generally that all the b's are powers and products of two of them (call them b_1 and b_2) corresponding to the same powers and products of $a_1^{(1)}$ and $a_2^{(1)}$.

19. To pass from the relations of $G^{(1)}$ given above to those of G deduced therefrom, $a_1^{(1)}$ and $a_2^{(1)}$ must be replaced respectively by b_1 and b_2, and an arbitrary

factor in a introduced (cf. No. 12). Doing so, it is seen that G is generated by elements a, b_1, b_2, satisfying the relations

$$\begin{aligned} a^p &= 1 \\ b_1^p &= a^{m_1} \\ b_2^p &= a^{m_2} \\ b_2 b_1 &= a^n b_1 b_2 \\ a b_i &= b_i a, \ i = 1,\ 2. \end{aligned}$$

From these relations follow readily

Formulæ of multiplication:

$$b_2^{\beta_2} b_1^{\beta_1} = a^{\beta_1 \beta_2 n} b_1^{\beta_1} b_2^{\beta_2}$$

$$(a^{\alpha} b_1^{\beta_1} b_2^{\beta_2})^q = a^{q\alpha + \frac{q(q-1)}{2} \beta_1 \beta_2 n} b_1^{q\beta_1} b_2^{q\beta_2}.$$

If $n \equiv 0 \pmod{p}$, then $b_2 b_1 = b_1 b_2$ and the group is commutative, and not of the type in question. Hence $n \not\equiv 0 \pmod{p}$.

If the given relations are transformed by all the generating elements no new relations are found. The only relations consequent upon the given relations are, therefore, their products and powers.

20. If
$$\begin{aligned} m_1 &= 0,\ 1,\ 2, \ldots . p-1 \\ m_2 &= 0,\ 1,\ 2, \ldots . p-1 \\ n &= 1,\ 2 \ldots\ldots . p-1, \text{ independently,} \end{aligned}$$

all the groups of the type are generated, and every such set of values used as exponents in the generating relations leads to a group of the type. For the relations suffice to reduce any expression of the form

$$a_1^{\alpha_1} b_1^{\beta_{11}} b_2^{\beta_{12}} a_1^{\alpha_2} b_1^{\beta_{21}} b_2^{\beta_{22}} \ldots . \ a_1^{\alpha_2} b_1^{\beta_{21}} b_2^{\beta_{22}}$$

to the form $a_1^{\alpha} b_1^{\beta_1} b_2^{\beta_2}$, $(\alpha,\ \beta_1,\ \beta_2 < p)$. Therefore every element of the group is given at least once by the expression just written if $\alpha, \beta_1, \beta_2 = 0,\ 1,\ 2 \ldots . p-1$, independently. The group is of order p^3 if all these elements are distinct. If two of the elements so found were equal, e. g. if

$$a^{\alpha_1} b_1^{\beta_{11}} b_2^{\beta_{12}} = a^{\alpha_2} b_1^{\beta_{21}} b_2^{\beta_{22}},$$

it follows that

$$a^{\alpha_1 - \alpha_2} b_1^{\beta_{11} - \beta_{21}} b_2^{\beta_{12} - \beta_{22}} = 1.$$

Unless $\alpha_1 = \alpha_2$, $\beta_{11} = \beta_{21}$, $\beta_{12} = \beta_{22}$, this is a new relation (not a product of those already given) which the generating elements satisfy. But we have seen that no such relation exists. Hence the group generated is actually of order p^3.*

21. It remains to determine for what sets of values of m_1, m_2, n, the groups are identical. To this end, we select in the group G for which m_1, m_2, n have a particular set of values, all the different systems of elements which will generate the group G. For each such system the values of m_1, m_2, n will, as a rule, be different, and the totality of these sets of values is the totality of the values of m_1, m_2, n leading to the group G. We shall thus distinguish all the different admissible sets of values of m_1, m_2, n into classes such that every set of a class, when used as exponents in the generating relations, leads to the same group, and that no two sets belonging to different classes lead to the same group. There will then be just as many different groups as there are classes of values of m_1, m_2, n. We shall find that the classes can be completely distinguished by certain functions of m_1, m_2, n which are invariant for each class, but may vary from class to class.

22. In the group G (defined in Nos. 18, 19) we now make the most general choice of a system of generating elements, a', b_1', b_2', viz.

$$
\begin{aligned}
a' &= a^{\delta} b_1^{\alpha_1} b_2^{\alpha_2} \\
b_i' &= a^{\gamma_i} b_1^{\beta_{i_1}} b_2^{\beta_{i_2}} \qquad\qquad i = 1,\ 2.
\end{aligned}
$$

As has been seen (Nos. 18–20), in order that these elements may be a system of generating elements of G they must satisfy relations of the form given in No. 19, and no others not products of these.† That is, we must have

$$
\begin{aligned}
a'^{p} &= 1 \\
b_i'^{p} &= a'^{m},\ i = 1,\ 2 \\
b_2' b_1' &= a'^{n'} b_1' b_2' \\
a' b_i' &= b_i' a',\ i = 1,\ 2.
\end{aligned}
$$

---

* In the same way it appears in every type subsequently to be considered, and in general, that the given relations with their products and powers are alone sufficient to reduce the group generated to the proper order; that therefore relations that are not products of the given relations reduce the order of the group further, and are hence inadmissible. If (as sometimes happens) relations not products of those given are consequences of them for particular values of the exponents, these values of the exponents, as not leading to a group of the type in question, must be excluded from consideration.

† The group *may* be generated by systems of elements satisfying relations quite different from these, but such systems need not be considered. For we have seen that every group of the type can be generated by a system of elements which does satisfy relations of the form given, and hence if we confine our attention to systems of the latter sort, we shall not thereby have excluded any groups from consideration.

If now the values of $a'b'_i$ in terms of a, b_1, b_2 be substituted, it appears that in order that the relation $a'b'_i = b'_i a'$ may hold it is necessary and sufficient that $\alpha_1 \equiv \alpha_2 \equiv 0 \pmod{p}$.

We may write then

$$a' = a^{\delta}$$
$$b'_i = a^{\gamma}\, b_1^{\beta_{i1}} b_2^{\beta_{i2}}, \quad i = 1,\ 2.$$

23. In order that the elements a', b'_i may generate the group G_1 it is necessary and sufficient that the elements a, b_i which, by hypothesis, generate G_1 be expressible in terms of a', b'_i. *I. e.*, the following relations must exist:

$$a = a'^{\delta'}$$
$$b_i = a'^{\gamma'_i} b_1'^{\beta'_{i1}} b_2'^{\beta'_{i2}}, \quad i = 1,\ 2.$$

Whence, substituting the values of a', b'_i,

$$a = a^{\delta\delta'}$$
$$b_i = a^{\delta\gamma'_i + f_i(\gamma_1,\, \gamma_2,\, \beta\text{'s})} . b_1^{\beta'_{i1}\beta_{11} + \beta'_{i2}\beta_{21}} . b_2^{\beta'_{i1}\beta_{12} + \beta'_{i2}\beta_{22}},$$

f_i being a polynomial whose precise form is not material here.
From these:

$$\begin{aligned} \delta\delta' &\equiv 1 \pmod{p} \\ \delta\gamma'_i + f_i(\gamma_1, \gamma_2, \beta\text{'s}) &\equiv 0 \pmod{p}, \quad i = 1,\ 2. \\ \beta'_{11}\beta_{11} + \beta'_{12}\beta_{21} &\equiv 1 \ (\quad\text{"}\quad) \\ \beta'_{11}\beta_{12} + \beta'_{12}\beta_{22} &\equiv 0 \ (\quad\text{"}\quad) \\ \beta'_{21}\beta_{11} + \beta'_{22}\beta_{21} &\equiv 0 \ (\quad\text{"}\quad) \\ \beta'_{21}\beta_{12} + \beta'_{22}\beta_{22} &\equiv 1 \ (\quad\text{"}\quad) \end{aligned}$$

The integers δ, γ_i, β_{ij} must be so chosen that values of the integers δ', γ'_i, β'_{ij} can be found which will satisfy this system of congruences. To this end, it is necessary and sufficient that the following conditions be satisfied:

$$\delta \not\equiv 0 \pmod{p}$$
$$\begin{vmatrix} \beta_{11} \beta_{12} \\ \beta_{21} \beta_{22} \end{vmatrix} \not\equiv 0 \ (\quad\text{"}\quad)$$

No restriction upon γ_1, γ_2 follows, since, whatever their values may be, values of γ'_i can always be found to satisfy the congruences in which γ_1, γ_2 appear.

24. *Notation.*[*]—The symbol $|\alpha|$ shall be used permanently to denote the determinant of the numbers α_{ij}, $i, j = 1,\ 2 \ldots . n$.

---

[*] Cf. Smith, Phil. Trans. 1861, p. 293.

If now we choose as generating elements

$$\begin{aligned} a' &= a^{\delta} \\ b'_i &= a^{\gamma} b_1^{\beta_{i1}} b_2^{\beta_{i2}}, \quad i = 1, 2 \\ \delta &\not\equiv 0, \ |\beta| \not\equiv 0 \pmod{p}, \end{aligned}$$

the group G will be generated. Substituting these values in the set of relations given in No. 22, the latter reduce to the following, (provided $p > 2$, which we assume hereafter to be the case, reserving the case $p = 2$ for separate consideration):

$$a^{m_1\beta_{i1} + m_2\beta_{i2}} = a^{\delta m'} \quad i = 1, 2.$$

$$a^{n(\beta_{11}\beta_{22} - \beta_{12}\beta_{21})} b_1^{\beta_{11} + \beta_{21}} b_2^{\beta_{12} + \beta_{22}} = a^{\delta n'} b_1^{\beta_{11} + \beta_{21}} . b_2^{\beta_{12} + \beta_{22}}.$$

Whence, if $\bar{\delta}$ be defined by $\bar{\delta}\delta \equiv 1 \pmod{p}$,

$$\begin{aligned} m'_i &\equiv \bar{\delta}(m_1\beta_{i1} + m_2\beta_{i2}) \pmod{p}, \ i = 1, 2. \\ n' &\equiv \bar{\delta}|\beta| n \qquad (\quad \text{“} \quad) \end{aligned}$$

By these formulæ are determined all the sets of values of m'_1, m'_2, n' which, when used as exponents in the generating relations, lead to the same group as m_1, m_2, n.

25. The choice of other generating elements for the group may be called a transformation of the group into itself, and the formulæ just written are the corresponding formulæ of transformation for the exponents. Those different sets of values of m_1, m_2, n, and those only, which can be transformed into each other by these formulæ characterize the same group. One of these sets of values may be selected as typical of them all and called the "reduced" set of values. The distinct groups are determined when, by these formulæ, several sets of reduced values are found such that no reduced set can be transformed into any other reduced set, but such that every admissible set of values of m_1, m_2, n can be transformed into one and only one of the reduced sets of values.

26. *Definition.*—An *invariant* of a type is a function of the variable exponents occurring in the generating relations of the type, which remains unaltered in value under any admissible transformation. Two groups for which an invariant has different values cannot be identical because they cannot be transformed into each other by the method just explained.

27. Since neither δ, $|\beta|$, nor n is $\equiv 0$, (mod p), it is always possible to choose δ and $|\beta|$ so that $n' \equiv 1$ (mod p). This is done, for instance, by putting

$$\delta \equiv n, \ |\beta| \equiv \begin{vmatrix} 10 \\ 01 \end{vmatrix} (\text{mod } p)^*$$

when

$$m_i' \equiv \bar{n} m_i, \quad i = 1, 2, \quad n' \equiv 1 \ (\text{mod } p).$$

This means that if a group be characterized by exponents m_1, m_2, n, it can always, by a different choice of generating elements, be expressed in a form having the exponents $\bar{n}m_1$, $\bar{n}m_2$, 1, i. e. by

$$\begin{aligned} a^p &= 1 \\ b_i^p &= a^{\bar{n}m}, \quad i = 1, 2, \\ b_2 b_1 &= a b_1 b_2. \end{aligned}$$

Since all groups of the type are contained in this form, we confine our attention hereafter to groups in which $n \equiv 1$ (mod p) and apply only such transformations as will leave n unaltered. This is no restriction upon the generality of the treatment.

Since by the results of No. 24, m_i' can be expressed linearly and homogeneously in terms of m_i (mod p), and conversely, it follows that the greatest common divisor of m_1, m_2 and p remains unaltered under any transformation, i. e. G.C.D. $m_1, m_2, p =$ G.C.D. m_1', m_2', p.

28. *Notation.*†—Denote the greatest common divisor of $a, b, \ldots . l$, by $[a, b, \ldots . l]$.

$A = [m_1, m_2, p]$ is then an *invariant* of the type. That two groups be identical it is *necessary* that A have the same value for each. We proceed to show that it is also *sufficient.*

A may have the values 1 and p. If $A = 1$, i. e. m_1 and m_2 are not both $\equiv 0$ (mod p), δ and β_{ij} can always be so chosen that

$$\begin{aligned} m_1'' &\equiv \bar{\delta}(m_1'\beta_{11} + m_2'\beta_{12}) \equiv \bar{n}\bar{\delta}(m_1\beta_{11} + m_2\beta_{12}) \equiv 1 \ (\text{mod } p) \\ m_2'' &\equiv \bar{\delta}(m_1'\beta_{21} + m_2'\beta_{22}) \equiv \bar{n}\bar{\delta}(m_1\beta_{21} + m_2\beta_{22}) \equiv 0 \ (\quad \text{``} \quad ) \\ n'' &\equiv \bar{\delta}\,|\beta|\,n' \equiv \bar{\delta}\,|\beta| \equiv 1 \qquad\qquad\qquad\qquad\quad (\quad \text{``} \quad). \end{aligned}$$

---

* This notation means that the elements of $|\beta|$ are respectively congruent (mod p) to the values written.

† Smith, Phil. Trans. 1861, p. 321.

I. e., if $A = 1$, all the sets of values of m_i n admissible under this restriction can be reduced to $m_1 \equiv 1$, $m_2 \equiv 0$, $n \equiv 1 \pmod{p}$. In other words, all the different sets of values of m_i, n for which $A = 1$, lead to the same group. When $A = p$, there is only one set of values of m_i admissible, viz. $m_1 \equiv m_2 \equiv 0 \pmod{p}$. There are then only two distinct groups according as $A = 1$ or $A = p$.

We take as reduced values

$$A = 1,\ m_1 \equiv 1,\ m_2 \equiv 0,\ n \equiv 1 \pmod{p}$$
$$A = p,\ m_1 \equiv 0,\ m_2 \equiv 0,\ n \equiv 1 \ (\quad \text{"} \quad).$$

The groups themselves are generated by elements satisfying the relations:

$(A = 1)$	$(A = p)$
$a^p = 1$	$a^p = 1$
$b_1^p = a$	$b_1^p = 1$
$b_2^p = 1$	$b_2^p = 1$
$b_2 b_1 = a b_1 b_2$	$b_2 b_1 = a b_1 b_2$
$a b_i = b_i a \quad i = 1,\ 2$	$a b_i = b_i a \quad i = 1,\ 2.$

29. *Case* $p = 2$.

When $p = 2$, instead of the results of No. 24, the following relations are deduced in a similar manner; (remembering that since $\delta \not\equiv 0 \pmod{p = 2}$ $|\beta| \not\equiv 0$, $n \not\equiv 0 \pmod{2}$ we have $\delta \equiv \bar{\delta} \equiv 1$, $n \equiv 1$, $|\beta| \equiv 1 \pmod{2}$):

$$m_i' \equiv \beta_{i1}\beta_{i2} + \beta_{i1}m_1 + \beta_{i2}m_2 \pmod{2},$$
$$n' \equiv n \equiv 1 \qquad\qquad (\quad \text{"} \quad).$$

If $\qquad m_1 \equiv m_2 \equiv 1 \pmod{2}$ then

$$m_1' \equiv \beta_{11}\beta_{12} + \beta_{11} + \beta_{12} \pmod{2}$$
$$m_2' \equiv \beta_{21}\beta_{22} + \beta_{21} + \beta_{22} \pmod{2}.$$

Since $|\beta| \equiv 1 \pmod{2}$, β_{i1} and β_{i2} are not both $\equiv 0 \pmod{2}$, and hence necessarily

$$m_1' \equiv m_2' \equiv 1 \pmod{2}.$$

Since the transformation is invertible $m_1 m_2$ remains unaltered (mod 2) under any admissible transformation. I. e., $A \equiv m_1 m_2 \pmod{2}$ is an invariant. We have considered above the case $A \equiv 1 \pmod{2}$. If $A \equiv 0 \pmod{2}$ at least one m is $\equiv 0 \pmod{2}$, and the β's can always be so chosen that $m_1' \equiv m_2' \equiv 0 \pmod{2}$.

There are then two groups according as $A \equiv 0$ or $A \equiv 1 \pmod{2}$.

30. *Groups of order* p^4.

$$\textit{Types}:\quad \text{I.}\quad \left.\begin{array}{r}(1111)\\(211)\\(22)\\(31)\\(4)\end{array}\right\}\ \text{The commutative groups.}$$

II. $(1\between 111)$
III. $(2\between 11)$
IV. $(1\between 21)$
V. $(11\between 11)$
VI. $(1\between 1\between 11)$.

31. *Type* $(1\between 111)$.

By the methods already used, (Nos. 18, 19), this type is seen to be generated by elements satisfying the relations:

$$\begin{aligned} &a^p = 1\\ &b_i^p = a^{m_i},\quad i = 1,\ 2,\ 3\\ &b_jb_i = a^{n_{ij}}b_ib_j,\quad i, j = 1,\ 2,\ 3 \text{ independently.}\\ &ab_i = b_ia,\quad i = 1,\ 2,\ 3. \end{aligned}$$

From the third relation it follows that

$$n_{ij} \equiv - n_{ji},\quad n_{ii} \equiv 0 \pmod p.$$

No new relations are found by transforming the above relations.

Formulæ of multiplication:

$$b_j^{\beta_2}b_i^{\beta_1} = a^{\beta_1\beta_2 n_{ij}}b_i^{\beta_1}b_j^{\beta_2}$$

$$(a^\alpha b_1^{\beta_1}b_2^{\beta_2}b_3^{\beta_3})^q = a^{q\alpha + \frac{q(q-1)}{2}\sum\limits_{j=i+1}^{3}\sum\limits_{i=1,2}\beta_i\beta_j n_{ij}} . b_1^{q\beta_1}b_2^{q\beta_2}b_3^{q\beta_3}.$$

32. *Condition* that no element except a and its powers be commutative with every element of the group. That $c = a^\alpha b_1^{\gamma_1}b_2^{\gamma_2}b_3^{\gamma_3}$ be commutative with every element of the group, it is necessary and sufficient that

$$cb_i = b_ic,\quad i = 1,\ 2,\ 3.$$

Substituting the value of c in this relation and reducing by the formulæ for multiplication, we find that it reduces to

$$a^{\sum\limits_{j=i+1}^{3} \gamma_j n_{ij}} = a^{\sum\limits_{j=1}^{i-1} \gamma_j n_{ji}} \quad i = 1,\ 2,\ 3.$$

Whence

$$\sum_{j=i+1}^{3} \gamma_j n_{ij} \equiv \sum_{j=1}^{i-1} \gamma_j n_{ji} \pmod{p} \quad i = 1,\ 2,\ 3,$$

or, remembering that $n_{ji} \equiv - n_{ij}$, $n_{ii} \equiv 0 \pmod{p}$,

$$\sum_{j=1}^{3} \gamma_j n_{ij} \equiv 0 \pmod{p} \quad i = 1,\ 2,\ 3.$$

In order that none but a and its powers may be commutative with every element of the whole group, the system of congruences last written must have no other solutions than

$$\gamma_1 \equiv \gamma_2 \equiv \gamma_3 \equiv 0 \pmod{p}.$$

The n's must therefore be so chosen that the system of congruences can be satisfied only by these values of γ_i. The condition for this is:

$$|n| \not\equiv 0 \pmod{p}.$$

But $|n|$ is a skew-symmetric determinant of odd order and hence*

$$|n| \equiv 0 \pmod{p}.$$

The type is therefore non-existent.

33. *Type* (2)(11).

By the previous methods (Nos. 18, 19), it is found that this type is generated by elements a, b_1, b_2, satisfying the relations:

$$\begin{aligned} a^{p^2} &= 1 \\ b_1^p &= a^{m_1} \\ b_2^p &= a^{m_2} \\ b_2 b_1 &= a^n b_1 b_2 \\ a b_i &= b_i a, \quad i = 1,\ 2. \end{aligned}$$

---

* Baltzer, Determinanten, §5, 8.

Formulæ of multiplication:

$$b_2^{\beta_2} b_1^{\beta_1} = a^{\beta_1\beta_2 n} b_1^{\beta_1} b_2^{\beta_2}$$

$$(a^{\alpha} b_1^{\beta_1} b_2^{\beta_2})^q = a^{q\alpha + \frac{q(q-1)}{2}\beta_1\beta_2 n} . b_1^{q\beta_1} . b_2^{q\beta_2} .$$

Relations consequent on these by transformation. Transforming the second relation written by b_2, and reducing by the multiplication formulæ, we have

$$a^{np} b_1^p = a^{m_1} ;$$

whence

$$a^{np} = 1 .$$

Accordingly, that this may not be a new relation satisfied by a, n must be so chosen that (v. note to No. 20)

$$np \equiv 0 \pmod{p^2}$$
$$n \equiv 0 \pmod{p} .$$

The condition that no element other than a and its powers be commutative with every element of the group is seen, by the method of No. 32, to be

$$n \not\equiv 0 \pmod{p^2} .$$

Nothing further is found by transforming the remaining relations.

34. If, now, the following elements of the group be considered as generating elements

$$a' = a^{\delta}$$
$$b_i' = a^{\alpha_i} b_1^{\beta_{i1}} b_2^{\beta_{i2}} ,\ i = 1,\ 2,$$

it is proved, by the method already explained in detail (Nos. 21 to 23), that the necessary and sufficient condition that the group generated by a', b_i' be actually the group under consideration, and not a subgroup of it, are

$$\delta \not\equiv 0,\ |\beta| \not\equiv 0 \pmod{p},\ \alpha_i \text{ remaining entirely arbitrary.}$$

By the method explained in No. 24 are found the following

Formulæ of Transformation:

$$\bar{\delta}(p\alpha_i + \frac{p(p-1)}{2}\beta_{i1}\beta_{i2} n + \beta_{i1} m_1 + \beta_{i2} m_2) \equiv m_i' \pmod{p^2},\ i = 1,\ 2,$$
$$\bar{\delta} |\beta| n \equiv n' \pmod{p^2} .$$

Since both n and n' are necessarily divisible by p but not by p^2, we can always choose δ and $|\beta|$ so that $n' \equiv p \pmod{p^2}$, (e. g. by

$$\delta \equiv \frac{n}{p}, \ |\beta| \equiv \begin{vmatrix} 10 \\ 01 \end{vmatrix} \ (\mathrm{mod}\ p)).$$

It appears from the form of the first formula of transformation above that the G.C.D. of m_1, m_2, p is an invariant, and that by a proper choice of the arbitrary quantity α_i, m_i' can always be made less than p. Since n is divisible by p, the case $p = 2$ is included in the general case.

We distinguish then

$$A = [m_1, m_2, p] = 1, \text{ and } A = p.$$

If $A = 1$, β_{ij} can always, as in the type (1)(11) (No. 28), be so chosen that $m_1 \equiv 1$, $m_2 \equiv 0 \pmod{p}$, and by giving the arbitrary quantity α_i a suitable value, we can always make $m_1' \equiv 1$, $m_2' \equiv 0 \pmod{p^2}$; while if $A = p$, i. e. if $m_1 \equiv m_2 \equiv 0 \pmod{p}$, we can always, by a proper choice of α_i, make $m_1' \equiv m_2' \equiv 0 \pmod{p^2}$. There are therefore two groups of this type, according as

$$A = 1, \text{ or } A = p.$$

35. *Type* (1)(21).

This type is generated by elements a, b_1, b_2, satisfying the relations:

$$\begin{aligned} a^p &= 1 \\ b_1^{p^2} &= a^{m_1} \\ b_2^p &= a^{m_2} \\ b_2 b_1 &= a^n b_1 b_2 \\ a b_i &= b_i a, \quad i = 1, \ 2. \end{aligned}$$

Formulæ of multiplication:

$$b_2^{\beta_2} b_1^{\beta_1} = a^{\beta_1 \beta_2 n} b_1^{\beta_1} b_2^{\beta_2}$$

$$(a^\alpha b_1^{\beta_1} b_2^{\beta_2})^q = a^{q\alpha + \frac{q(q-1)}{2} \beta_1 \beta_2 n} . \, b_1^{q\beta_1} b_2^{q\beta_2}.$$

By the formulæ of multiplication,

$$\begin{aligned} b_2 b_1^p &= a^{pn} b_1^p b_2 \\ \text{or} \quad b_2 b_1^p &= b_1^p b_2. \end{aligned}$$

That is, b_1^p is commutative with b_2, and being already commutative with itself and with a, it is commutative with every element of the group. This is contrary to the hypothesis that a and its powers constitute the totality of the elements commutative with every element of the group. There are therefore no groups of this type.

36. *Type* (11)(11).

By the previous methods, this type is seen to be generated by elements a_1, a_2, b_1, b_2, satisfying the relations

$$\left.\begin{aligned} a_i^p &= 1 \\ b_i^p &= a_1^{m_{i1}} a_2^{m_{i2}} \end{aligned}\right\} i = 1,\ 2.$$

$$b_2 b_1 = a_1^{n_1} a_2^{n_2} b_1 b_2$$

$$a_1 a_2 = a_2 a_1$$

$$a_i b_j = b_j a_i,\quad i, j = 1,\ 2 \text{ independently.}$$

Formulæ of multiplication:

$$b_2^{\beta_2} b_1^{\beta_1} = a_1^{\beta_1 \beta_2 n_1} . a_2^{\beta_1 \beta_2 n_2} . b_1^{\beta_1} . b_2^{\beta_2}$$

$$(a_1^{\alpha_1} a_2^{\alpha_2} b_1^{\beta_1} b_2^{\beta_2})^q = a_1^{q\alpha_1 + \frac{q(q-1)}{2} \beta_1 \beta_2 n_1} . a_2^{q\alpha_2 + \frac{q(q-1)}{2} \beta_1 \beta_2 n_2} . b_1^{q\beta_1} b_2^{q\beta_2}.$$

No new conditions are found by transforming the given relations by each of the generating elements.

In order that no element, other than powers and products of a_1, a_2, be commutative with every element of the group, it is shown as before (No. 32), to be necessary and sufficient that at least one of the quantities n_1, n_2 be not congruent zero, (mod p).

37. Just as before (Nos. 21–24), the conditions and formulæ of transformation are found. It is necessary to distinguish the cases $p > 2$ and $p = 2$.

Formulæ of transformation, $p > 2$.

$$\sum_{j=1,2} \beta_{ij} m_{j\kappa} \equiv \sum_{j=1,2} \delta_{j\kappa} m'_{ij} \pmod{p} \quad i, \kappa = 1,\ 2 \text{ independently.}$$

$$(\beta_{11}\beta_{22} - \beta_{12}\beta_{21}) n_i \equiv \delta_{1i} n'_1 + \delta_{2i} n'_2 \pmod{p} \quad i = 1,\ 2.$$

$$|\beta| \not\equiv 0,\quad |\delta| \not\equiv 0,\ (\text{mod } p).$$

From the second set of formulæ,

$$n_1' \equiv \overline{|\delta|} \cdot |\beta| \, (n_1\delta_{22} - n_2\delta_{21}), \ (\text{mod } p)$$
$$n_2' \equiv \overline{|\delta|} \cdot |\beta| \, (n_2\delta_{11} - n_1\delta_{12}), \ (\quad \text{``} \quad).$$

We choose the β's and δ's so that

$$n_1' \equiv 1, \ n_2' \equiv 0, \ (\text{mod } p).$$

Such a choice, for instance, is

$$|\beta| \equiv \begin{vmatrix} 10 \\ 01 \end{vmatrix}, \ (\text{mod } p)$$
$$|\delta| \equiv \begin{vmatrix} n_1 & n_2 \\ \delta_{21} & \delta_{22} \end{vmatrix} \equiv 1, \ (\text{mod } p).$$

With these values, the resulting values of m_{ij}' are

$$m_{11}' \equiv \begin{vmatrix} m_{11} & \delta_{21} \\ m_{12} & \delta_{22} \end{vmatrix}, \ (\text{mod } p),$$
$$m_{12}' \equiv \begin{vmatrix} n_1 & m_{11} \\ n_2 & m_{12} \end{vmatrix}, \ (\quad \text{``} \quad),$$
$$m_{21}' \equiv \begin{vmatrix} m_{21} & \delta_{21} \\ m_{22} & \delta_{22} \end{vmatrix}, \ (\quad \text{``} \quad),$$
$$m_{22}' \equiv \begin{vmatrix} n_1 & m_{21} \\ n_2 & m_{22} \end{vmatrix}, \ (\quad \text{``} \quad).$$

In applying any further transformation we must have, in order to leave the n's unaltered,

$$|\beta| \equiv \delta_{11}, \ \delta_{12} \equiv 0, \ (\text{mod } p).$$

$A = [|m|, p]$ is invariant. This is proved by applying to the m's the most general transformation admissible. The determinant of the m''s is found to differ from that of the m's by a factor which is not congruent zero, (mod p). Hence A remains unaltered.

38. Suppose $A = 1$, i. e. $|m| \not\equiv 0$ (mod p). Applying to the m''s the most general transformation leaving the n''s unaltered, the result is (see conditions above):

$$m_{11}'' \equiv \overline{|\beta|} \, \{\beta_{11}m_{11}' + \beta_{12}m_{21}' - \delta_{21}\bar{\delta}_{22}(\beta_{11}m_{12}' + \beta_{12}m_{22}')\} \ (\text{mod } p),$$
$$m_{21}'' \equiv \overline{|\beta|} \, \{\beta_{21}m_{11}' + \beta_{22}m_{21}' - \delta_{21}\bar{\delta}_{22}(\beta_{21}m_{12}' + \beta_{22}m_{22}')\} \ (\quad \text{``} \quad),$$
$$m_{12}'' \equiv \bar{\delta}_{22}(\beta_{11}m_{12}' + \beta_{12}m_{22}') \qquad (\quad \text{``} \quad),$$
$$m_{22}'' \equiv \bar{\delta}_{22}(\beta_{21}m_{12}' + \beta_{22}m_{22}') \qquad (\quad \text{``} \quad).$$

Choose $|\beta| \equiv \begin{vmatrix} m'_{22}, & -m'_{12} \\ -m'_{21}, & m'_{11} \end{vmatrix}$, $\delta_{21} \equiv 0$, $\delta_{22} \equiv |m|$, (mod p)

then $m''_{11} \equiv 1$, $m''_{12} \equiv 0$, (mod p),
$m''_{21} \equiv 0$, $m''_{22} \equiv 1$, (").

I. e., all values whatever of the m's, subject to the condition that $|m| \not\equiv 0$ (mod p) can be reduced to the set just written, by a transformation leaving $n_1 \equiv 1$, $n_2 \equiv 0$. There is hence but one group when $A = 1$.

39. Suppose $A = p$, i. e., $|m| \equiv 0$ (mod p). In deducing the first four congruences of No. 38, no assumption was made as to whether or not $|m| \equiv 0$ (mod p). These formulæ, therefore, hold true also in the present case. On the face of the formulæ it is evident that $B = [m'_{12}, m'_{22}, p]$ remains unaltered by this transformation. When the values of m'_{12} and m'_{22} in terms of the original parameters are substituted, we must have an invariant of the type. For if

$$B = \left[\begin{vmatrix} n_1, & m_{11} \\ n_2, & m_{12} \end{vmatrix}, \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix}, p \right]$$

is not invariant, it is possible by some admissible transformation applied to n_1, n_2, m_{ij}, to reach values $n_1^{(1)}$, $n_2^{(1)}$, $m_{ij}^{(1)}$, such that $B^{(1)} \neq B$. When now $n_1^{(1)}$ is made unity and $n_2^{(1)}$ zero (mod p), $m_{12}^{(1)'}$ and $m_{22}^{(1)'}$ are the determinants in $B^{(1)}$. By the hypothesis that $B^{(1)} \neq B$, they have not the same G.C.D. with p as the determinants in B.

Therefore, supposing B *not* an invariant of the type, it is possible by three transformations, viz. from m'_{ij} back to m_{ij}, then to $m_{ij}^{(1)}$, then to $m_{ij}^{(1)'}$, (and these transformations can be combined into one leaving $n'_1 \equiv 1$, $n'_2 \equiv 0$, (mod p)) to alter $B = [m'_{12}, m'_{22}, p]$. But this last has been shown to be impossible. Hence B is an invariant of the type.

40. The same reasoning shows generally that if, after having applied any number of particular transformations, any function of the resulting parameters remains unaltered under every transformation which does not affect the results of the previous transformations, then, when the transformed parameters are replaced by their values in terms of the original parameters, the resulting expression is an invariant of the type.

41. That B is an invariant can also be verified by applying to it the most general admissible transformation, when it appears that B remains unaltered.

We distinguish now $B=1$, and $B=p$. Case $B=1$. As a particular transformation we choose,

$$|\beta| \equiv \begin{vmatrix} m'_{22}, & -m'_{12} \\ \beta_{21} & \beta_{22} \end{vmatrix} \equiv 1, \quad \begin{array}{l} \delta_{22} \equiv 1 \pmod{p}, \\ \delta_{21} \equiv \beta_{21} m'_{11} + \beta_{22} m'_{21}, \pmod{p}, \end{array}$$

while we have in addition (No. 37) the conditions $\delta_{11} \equiv |\beta| \equiv 1$, $\delta_{12} \equiv 0$ (mod'p)·

These values, substituted in the congruences of No. 38 give, (remembering that $|m| \equiv 0 \pmod{p}$),

$$\begin{array}{ll} m''_{11} \equiv \overline{|\beta|}\,(m'_{22} m'_{11} - m'_{12} m'_{21}) \equiv 0 & \pmod{p} \\ m''_{21} \equiv 0, \ m''_{12} \equiv 0, \ m''_{22} \equiv 1 & (\quad\text{"}\quad). \end{array}$$

There is then only one group in case $A=p$, $B=1$.

If $B=p$, i. e. $m'_{12} \equiv m'_{22} \equiv 0$, (mod p) we must distinguish whether or not $m'_{11} \equiv m'_{21} \equiv 0 \pmod{p}$. This leads to a new invariant, viz.

$$C = [m_{11}, m_{12}, m_{21}, m_{22}, p].$$

That this is invariant appears from the first formula of No. 37, remembering that $|\delta| \equiv\!|\!\equiv 0 \pmod{p}$.

If $B=p$, $C=1$, we make $m''_{11} \equiv 0$, $m''_{21} \equiv 1 \pmod{p}$, (No. 38).

If $B=p$, $C=p$, then necessarily

$$m''_{11} \equiv m''_{21} \equiv 0 \pmod{p}.$$

We have now found three invariants of the type. We have proved that all the groups characterized by any one of the possible combinations of values of the invariants are identical. Two groups whose invariants do not coincide in value cannot be identical. We have then reached a complete system of invariants which defines every group of the type once and only once when the invariants take all possible values.

Groups, Type $(11 \between 11)$, $p > 2$.

1.)	2.)	3.)	4.)
$A=1$,	p,	p,	p,
$B=1$,	1,	p,	p,
$C=1$,	1,	1,	p.

42. *Type* $(11)(11)$, $p = 2$.

In this case we find as before the *formulæ of transformation:*

$$\beta_{i1}\beta_{i2}n_\kappa + \beta_{i1}m_{1\kappa} + \beta_{i2}m_{2\kappa} \equiv m'_{i1}\delta_{1\kappa} + m'_{i2}\delta_{2\kappa} \pmod 2, \quad i, \varkappa = 1,\ 2, \text{ independently.}$$

$$(\beta_{11}\beta_{22} - \beta_{12}\beta_{21})n_\kappa \equiv \delta_{1\kappa}n'_1 + \delta_{2\kappa}n'_2 \pmod 2, \quad \varkappa = 1,\ 2.$$

$$|\delta| \not\equiv 0, \quad |\beta| \not\equiv 0 \pmod 2 \; \therefore |\delta| \equiv |\beta| \equiv 1 \pmod 2.$$

At least one of the integers $n_1 n_2$ is $\not\equiv 0 \pmod 2$. From the second formula of transformation,

$$n'_1 \equiv \begin{vmatrix} n_1 & \delta_{21} \\ n_2 & \delta_{22} \end{vmatrix} \pmod 2,$$

$$n'_2 \equiv \begin{vmatrix} \delta_{11} & n_1 \\ \delta_{12} & n_2 \end{vmatrix} \; (\;``\;)$$

$$\text{Choose } \delta \equiv \begin{vmatrix} n_1, & n_2 \\ n_1 + n_2, & n_1 \end{vmatrix}, \quad |\beta| \equiv \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \pmod 2.$$

This makes $n'_1 \equiv 1$, $n'_2 \equiv 0$, (mod 2), irrespective of the values of n_1 and n_2. The resulting values of m'_{ij} are

$$m'_{11} \equiv \begin{vmatrix} m_{11}, & n_1 + n_2 \\ m_{12}, & n_1 \end{vmatrix} \pmod 2,$$

$$m'_{12} \equiv \begin{vmatrix} n_1, & m_{11} \\ n_2, & m_{12} \end{vmatrix} \; (\;``\;),$$

$$m'_{21} \equiv \begin{vmatrix} m_{21}, & n_1 + n_2 \\ m_{22}, & n_1 \end{vmatrix} \; (\;``\;),$$

$$m'_{22} \equiv \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix} \; (\;``\;).$$

The most general transformation leaving the values $n_1 \equiv 1$, $n_2 \equiv 0$ (mod 2) unaltered is

$$|\delta| \equiv \begin{vmatrix} 1 & 0 \\ \delta_{21} & 1 \end{vmatrix}, \quad |\beta| \text{ arbitrary.}$$

Applying this transformation we find that

$$m''_{11} \equiv \beta_{11}\beta_{12} + \beta_{11}m'_{11} + \beta_{12}m'_{21} + \delta_{21}(\beta_{11}m'_{12} + \beta_{12}m'_{22}) \pmod 2,$$
$$m''_{21} \equiv \beta_{21}\beta_{22} + \beta_{21}m'_{11} + \beta_{22}m'_{21} + \delta_{21}(\beta_{21}m'_{12} + \beta_{22}m'_{22}) \; (\;``\;),$$
$$m''_{12} \equiv \beta_{11}m'_{12} + \beta_{12}m'_{22} \pmod 2,$$
$$m''_{22} \equiv \beta_{21}m'_{12} + \beta_{22}m'_{22} \; (\;``\;).$$

43. Since m''_{12} and m''_{22} are expressible linearly and homogeneously in terms of m'_{12} and m'_{22} and conversely, it follows that $[m'_{12}, m'_{22}, 2]$ remains invariant

under this, the most general transformation leaving $n'_1 \equiv 1$, $n'_2 \equiv 0$, (mod 2) and that hence, in terms of the original parameters,

$$A \equiv \left[\begin{vmatrix} n_1, & m_{11} \\ n_2, & m_{12} \end{vmatrix}, \quad \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix}, \right] \pmod 2$$

is an invariant of the type according to the considerations of Nos. 39, 40. The fact that A is an invariant can also be verified by applying to A the most general transformation admissible, when it is found to remain unaltered. If, when $A \equiv 0$, $m'_{11} \equiv m'_{21} \equiv 1$, (mod 2), then necessarily, since $|\beta| \equiv 1$ (mod 2), $m''_{11} \equiv m''_{21} \equiv 1$, (mod 2). In this case, therefore, we must distinguish whether or not $m'_{11} \equiv m'_{21} \equiv 1$, (mod 2), and hence $m'_{11} . m'_{21}(A+1)$ is invariant. Put

$$B \equiv \begin{vmatrix} m_{11}, & n_1 + n_2 \\ m_{12}, & n_1 \end{vmatrix} . \begin{vmatrix} m_{21}, & n_1 + n_2 \\ m_{22}, & n_1 \end{vmatrix} . (A+1), \pmod 2 .$$

This is invariant according to the general theory, (Nos. 39, 40), as may also be verified by applying the most general transformation admissible.

We have just considered above the case $A \equiv 0$, $B \equiv 1$, (mod 2), while if $A \equiv 0$, $B \equiv 0$, (mod 2), we can always, by a proper choice of $|\beta|$ make $m''_{11} \equiv m''_{21} \equiv 0$ (mod 2). If $A \equiv 0$, there are therefore two groups according as $B \equiv 0, 1$ (mod 2).

Case $A \equiv 1$. In this case $B \equiv 0$ (mod 2) necessarily. Applying the transformation

$$|\beta| \equiv \begin{vmatrix} m'_{22}, & m'_{12} \\ m'_{22} + 1, & 1 \end{vmatrix}, \quad |\delta| \equiv \begin{vmatrix} 1, & 0 \\ \delta_{21}, & 1 \end{vmatrix} \pmod 2,$$

with the result:

$$\begin{aligned} & m''_{12} \equiv 0, \ m''_{22} \equiv 1 \pmod 2, \\ & m''_{11} \equiv m'_{12} m'_{22} + m'_{11} m'_{22} + m'_{12} m'_{21} \pmod 2, \\ & m''_{21} \equiv (m'_{22} + 1)(m'_{11} + 1) + m'_{21} + \delta_{21} \pmod 2 ; \end{aligned}$$

m''_{21} can always, by a proper choice of the arbitrary quantity δ_{21}, be made $\equiv 0$ (mod 2). We must distinguish, finally, whether or not $m''_{11} \equiv 0$ (mod 2). By previous methods, then,

$$\begin{aligned} C \equiv m''_{11} & \equiv m'_{12} m'_{22} + |m'| \\ & \equiv \begin{vmatrix} n_1 & m_{11} \\ n_2 & m_{12} \end{vmatrix} . \begin{vmatrix} n_1 & m_{21} \\ n_2 & m_{22} \end{vmatrix} + \begin{vmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{vmatrix} \pmod 2 \end{aligned}$$

is an invariant of the type, and distinguishes the two groups possible when $A \equiv 1$ (mod 2).

We have now considered all the possibilities, have reached a complete system of invariants and can enumerate thereby the groups of the type, viz.

Groups, Type $(11\between 11)$, $p = 2$.

	1.)	2.)	3.)	4.)
$A =$	0,	1,	1,	0,
$B =$	1,	0,	0,	0,
$C =$	0,	1,	0,	0.

44. *Type* $(1\between 1\between 11)$.

The groups of this type are generated by four elements, a, b, c_1, c_2, satisfying the relations:

$$\begin{aligned} a^p &= 1, \\ b^p &= a^m, \\ \left.\begin{aligned} c_i^p &= a^n b^{f_i}, \\ c_i b &= a^q b c_i, \end{aligned}\right\} & \; i = 1,\ 2. \\ c_2 c_1 &= a^t b^h c_1 c_2, \\ ab &= ba, \\ ac_i &= c_i a, \quad i = 1,\ 2. \end{aligned}$$

It is necessary that $h \mathrel{\equiv\!|\!\equiv} 0 \pmod{p}$. For otherwise the group $G^{(1)}$ whose relations are found (No. 12) by placing in the above relations $a = 1$ would be a commutative group, and not of type $(1\between 11)$ as it should be.

Formulæ of multiplication:

$$c_i^\sigma b^\rho = a^{\sigma\rho q_i} b^\rho c_i^\sigma,$$

$$c_2^\sigma c_1^\rho = a^{\sigma\rho\left[t + h\frac{(\sigma-1)q_2 + (\rho-1)q_1}{2}\right]} . b^{\rho\sigma h} c_1^\rho c_2^\sigma,$$

$$(b^\beta c_1^{\gamma_1} c_2^{\gamma_2})^\tau = a^{\frac{\tau(\tau-1)}{2}\left\{\gamma_1\gamma_2\left[t + h\frac{(\gamma_1-1)q_1 - q_2}{2}\right] + (\gamma_1 q_1 + \gamma_2 q_2)\beta_1\right\} + \frac{\tau(\tau-1)(2\tau-1)}{6}h\gamma_1\gamma_2\left[\gamma_1 q_1 + \frac{\gamma_2 q_2}{2}\right]}$$
$$. b^{\frac{\tau(\tau-1)}{2}\gamma_2\gamma_1 h + \tau\beta} . c_1^{\tau\gamma_1} c_2^{\tau\gamma_2}.$$

It will be seen by the methods used previously that in order that no element except a and its powers be commutative with every element of the whole group, it is necessary and sufficient that not both q_1 and q_2 be congruent zero (mod p).

45. By transforming all the generating relations by each of the generating elements of the group, we find the complete system of relations consequent upon

the given relations. Nearly all of the relations resulting reduce to one or the other of those given, but the relations obtained by transforming the third relation given by c_i do not do so, and when $p > 2$, they are

$$\begin{aligned} a^{-mh+f_2q_1} &= 1, \\ a^{-mh+f_1q_2} &= 1, \\ a^{f_2q_2} &= 1, \\ a^{f_1q_1} &= 1. \end{aligned}$$

Hence, (see note to No. 20),

$$\begin{aligned} mh - f_2q_1 &\equiv 0 \pmod p, \\ mh - f_1q_2 &\equiv 0 \ (\text{''}), \\ f_2q_2 &\equiv 0 \ (\text{''}), \\ f_1q_1 &\equiv 0 \ (\text{''}). \end{aligned}$$

From these congruences it follows, since q_1 and q_2 are not both congruent zero, (mod p), that

$$m \equiv f_1 \equiv f_2 \equiv 0 \pmod p.$$

The case $p = 2$ is reserved for separate consideration.

Substituting these values, the generating relations become (provided $p > 2$):

$$\begin{aligned} & a^p = 1, \\ & b^p = 1, \\ & \left.\begin{aligned} c_i^p &= a^{n_i}, \\ c_ib &= a^{q_i}bc_i, \end{aligned}\right\} i = 1,\ 2. \\ & c_2c_1 = a^tb^hc_1c_2, \\ & ab = ba, \\ & ac_i = c_ia. \quad i = 1,\ 2. \end{aligned}$$

Subject to the restrictions $h \not\equiv 0$, q_1 and q_2 not both $\equiv 0$, (mod p), these relations define a group of our type for every set of values of n_i, q_i, t, h.

46. We now make the most general choice of generating elements a', b', c_i', as follows (cf. No. 22):

$$\begin{aligned} & a' = a^{\delta}, \\ & b' = a^{\epsilon}b^{\zeta}, \\ & c_i' = a^{\alpha_i}b^{\beta_i}c_1^{\gamma_{i1}}c_2^{\gamma_{i2}}, \quad i = 1,\ 2. \end{aligned}$$

In order that the group generated by a', b', c_i', be actually the group under consideration, and not a subgroup of it, it appears, by previous methods (No. 23), to be necessary and sufficient that the conditions

$$\delta \not\equiv 0,\ \zeta \not\equiv 0,\ |\gamma| \not\equiv 0 \pmod{p},$$

be satisfied.

At this point, distinction must be made between $p = 3$ and $p > 3$. Reserving the case $p = 3$ for subsequent consideration, it is found by previous methods (Nos. 22–25) that, when $p > 3$, the following are the

Formulæ of transformation:

$$h' \equiv \bar{\zeta}|\gamma|h \pmod{p},$$

$$\left.\begin{array}{l} n_i' \equiv \bar{\delta}(\gamma_{i1}n_1 + \gamma_{i2}n_2) \pmod{p}, \\ q_i' \equiv \bar{\delta}\zeta(\gamma_{i1}q_1 + \gamma_{i2}q_2)\ (\quad\text{``}\quad), \end{array}\right\} i = 1,\ 2,$$

$$\begin{aligned} t' \equiv \bar{\delta}\Big[\ |\gamma|t - \varepsilon\bar{\zeta}|\gamma|h + \Big\{h\Big[\frac{\gamma_{11}^2\gamma_{22} - \gamma_{12}\gamma_{21}^2 - |\gamma|}{2} + \gamma_{11}\gamma_{22}(\gamma_{22} - \gamma_{12})\Big] + \gamma_{21}\beta_1 - \gamma_{11}\beta_2\Big\}q \\ + \Big\{h\Big[\frac{\gamma_{11}\gamma_{22}^2 - \gamma_{21}\gamma_{12}^2 - |\gamma|}{2}\Big] + \gamma_{22}\beta_1 - \gamma_{12}\beta_2\Big\}q_2\Big]. \end{aligned}$$

47. Since ε is perfectly arbitrary, and appears only in the value of t' and is there multiplied by a factor which can never be congruent zero (mod p), it follows that, in every transformation, ε can (without affecting any quantity other than t') be given such a value that $t' \equiv 0 \pmod{p}$. We shall suppose throughout that this is done.

We first make $h' \equiv 1 \pmod{p}$ by the following transformation:

$$|\gamma| \equiv \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix},\ \varepsilon \equiv \beta_1 \equiv \beta_2 \equiv 0,\ \delta \equiv 1,\ \zeta \equiv h, \pmod{p}.$$

Results:

$$n_i' \equiv n_i,\ q_i' \equiv hq_i,\ t' \equiv t + hq_1,\ h' \equiv 1, \pmod{p}.$$

If now, considering the primed exponents as given, we apply the most general transformation such that $h'' \equiv h' \equiv 1 \pmod{p}$, the exponents of transformation are subject to the restriction $|\gamma| \equiv \zeta \pmod{p}$. The results of this transformation are

$$\begin{aligned} n_i'' &\equiv \bar{\delta}(\gamma_{i1}n_1' + \gamma_{i2}n_2') \equiv \bar{\delta}(\gamma_{i1}n_1 + \gamma_{i2}n_2) \pmod{p}, \\ q_i'' &\equiv \bar{\delta}\zeta(\gamma_{i1}q_1' + \gamma_{i2}q_2') \equiv \bar{\delta}\zeta h(\gamma_{i1}q_1 + \gamma_{i2}q_2)\ (\quad\text{``}\quad),\ i = 1,\ 2. \end{aligned}$$

Giving the exponents of transformation the following particular values,

$$\delta \equiv h, \; |\gamma| \equiv \begin{vmatrix} \gamma_{11}, & \gamma_{12} \\ -q_2, & q_1 \end{vmatrix} \equiv \zeta \equiv 1 \pmod{p},$$

we have

$$\begin{aligned} h'' &\equiv h' \equiv 1 && \pmod{p}, \\ n_i'' &\equiv \bar{h}(\gamma_{i1}n_1 + \gamma_{i2}n_2) && (\;\text{"}\;), \\ q_1'' &\equiv 1 && (\;\text{"}\;), \\ q_2'' &\equiv 0 && (\;\text{"}\;). \end{aligned}$$

Let $A = [n_1, n_2, p]$. It is necessary to distinguish whether or not $A \equiv 0 \pmod{p}$. A is invariant as appears from the form of the general relation between the n's and n''s. There is only one set of values for which $A \equiv 0 \pmod{p}$, viz. $n_1 \equiv n_2 \equiv 0 \pmod{p}$.

Suppose $A \equiv 1 \pmod{p}$. We had above

$$\begin{aligned} n_1'' &\equiv h(\gamma_{11}n_1 + \gamma_{12}n_2) \pmod{p}, \\ n_2'' &\equiv h(-q_2n_1 + q_1n_2) \equiv h \begin{vmatrix} q_1 & q_2 \\ n_1 & n_2 \end{vmatrix} \pmod{p}. \end{aligned}$$

In order to leave $q_1'' \equiv 1$, $q_2'' \equiv 0 \pmod{p}$ unaltered, any further transformation is subject to the additional conditions,

$$\gamma_{11} \equiv \delta\bar{\zeta}\bar{h}, \; \gamma_{21} \quad 0, \; \therefore \gamma_{22} \not\equiv 0 \pmod{p}.$$

As before $|\gamma| \equiv \zeta$, $\therefore \gamma_{22} = \zeta^2\delta h \pmod{p}$, γ_{12} quite arbitrary.

The results of the transformation are

$$\begin{aligned} n_1''' &\equiv \bar{\delta}(\delta\bar{\zeta}\bar{h}n_1'' + \gamma_{12}n_2'') && \pmod{p}, \\ n_2''' &\equiv \bar{\delta}\gamma_{22}n_2'' && (\;\text{"}\;), \end{aligned}$$

or,

$$\begin{aligned} n_1''' &\equiv \bar{\zeta}hn_1'' + \bar{\delta}\gamma_{12}h \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} && (\;\text{"}\;), \\ n_2''' &\equiv \bar{\delta}\gamma_{22}h \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} && (\;\text{"}\;), \\ &\equiv \zeta^2\bar{\delta}^2h^2 \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} && (\;\text{"}\;), \end{aligned}$$

If $\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \equiv 0 \pmod{p}$, then necessarily $n_2''' \equiv 0 \pmod{p}$. It is verified as before that $B \equiv \left[\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}, p \right]$ is an invariant.

If $A\equiv 1$, and $B\equiv 0 \pmod{p}$, then $n_1'' \not\equiv 0 \pmod{p}$. For $n_1''\equiv h(\gamma_{11}n_1+\gamma_{12}n_2)$ $\pmod{p}$, where the γ's satisfy also the congruence

$$\gamma_{11}q_1+\gamma_{12}q \equiv 1 \pmod{p};$$

since $A\equiv 1$, n_1 and n_2 are not both $\equiv 0 \pmod{p}$, and q_1 and q_2 are not both $\equiv 0 \pmod{p}$, and hence, since $\begin{vmatrix} q_1 & q_2 \\ n_1 & n_2 \end{vmatrix} \equiv 0 \pmod{p}$, the value of n_1'' just written is a non-vanishing multiple $\pmod{p}$ of the congruence $\gamma_{11}q_1+\gamma_{12}q_2\equiv 1 \pmod{p}$, and therefore, $n_1'' \not\equiv 0 \pmod{p}$.

Since $n_1'' \not\equiv 0 \pmod{p}$, ζ can always be so chosen that $n_1''' \equiv 1 \pmod{p}$.

In the case $A\equiv 1$, $B\equiv 0 \pmod{p}$, there is then but one group.

If $$A\equiv 1,\ B\equiv 1, \text{ i. e. } \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \not\equiv 0 \pmod{p},$$

then $$n_2''' \equiv (\zeta\bar{\delta}h)^2 \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \pmod{p}.$$

If $\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}$ is a quadratic residue of p, m_2''' can be made $\equiv 1 \pmod{p}$, while if $\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}$ is a quadratic non-residue of p, n_2''' can be reduced to any non-residue of p we please. Hence distinction must be made whether

$$C=\left(\frac{\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}}{p}\right)^{*} = \pm 1.$$

C is an invariant, as may be verified in the usual way. In either case, m_1''' is made zero by a proper choice of γ_{12} which is perfectly arbitrary.

A, B, C form, therefore, a complete system of invariants whereby are distinguished the following

Groups, Type (1)(1)(11), $p>3$.

	1.)	2.)	3.)	4.)
$A\equiv$	0,	1,	1,	1,
$B\equiv$	0,	0,	1,	1,
$C=$	$+1$,	$+1$,	$+1$,	-1.

---

* Legendre's symbol. Consider $\left(\frac{0}{p}\right)=+1$.

48. *Case* $p = 3$.

Formulæ of transformation:

$$
\begin{aligned}
&h' \equiv \bar{\zeta}\,|\gamma|\,h && (\text{mod } 3),\\
&q_i' \equiv \bar{\delta}\zeta(\gamma_{i1}q_1 + \gamma_{i2}q_2) && (\quad \text{``} \quad),\ i = 1,\ 2,\\
&n_i' \equiv \bar{\delta}\Big[\gamma_{i1}\gamma_{i2}h\left\{\frac{(\gamma_{i1} - 3)q_1 - (\gamma_{i2} + 3)q_2}{2}\right\} + \gamma_{i1}n_1 + \gamma_{i2}n_2\Big] && (\text{mod } 3),
\end{aligned}
$$

or, multiplying by 2 and rejecting multiples of 3,

$$n_i' \equiv \bar{\delta}\{\gamma_{i1}\gamma_{i2}h(\gamma_{i2}q_2 - \gamma_{i1}q_1) + \gamma_{i1}n_1 + \gamma_{i2}n_2\} \pmod 3,\ i = 1,\ 2.$$

The exponent t' has the same value as in the case $p > 3$, and just as in that case it is made zero by giving the arbitrary quantity ε a suitable value.

If $\alpha \not\equiv 0 \pmod 3$, then by Fermat's theorem, $\alpha^2 \equiv 1$ and $\bar{\alpha} \equiv \alpha \pmod 3$; throughout the case $p = 3$ we may therefore replace $\bar{\alpha}$ by α.

We first apply a transformation to make $h' \equiv 1 \pmod 3$, viz.

$\delta \equiv 1$, $\zeta \equiv h$, $|\gamma| \equiv \begin{vmatrix} 10 \\ 01 \end{vmatrix} \pmod 3$, with the result $n_i' \equiv n_i$, $q_i' \equiv hq_i$, $h' \equiv 1 \pmod 3$.
To make $q'' \equiv 1$, $q_2'' \equiv 0 \pmod 3$ we now apply the transformation

$$|\gamma| \equiv \begin{vmatrix} 2q_1q_2^2 + q_1, & q_2 \\ -q_2, & q_1 \end{vmatrix} \equiv 1,\ \zeta \equiv 1,\ \delta \equiv h \pmod 3,$$

with the results:

$$
\begin{aligned}
&h'' \equiv 1 && (\text{mod } 3),\\
&q_1'' \equiv 1 && (\quad \text{``} \quad),\\
&q_2'' \equiv 0 && (\quad \text{``} \quad),\\
&n_1'' \equiv h[(2q_1q_2^2 + q_1)n_1 + q_2n_2] && (\text{mod } 3),\\
&n_2'' \equiv q_1^2q_2^2 + h\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} && (\quad \text{``} \quad)
\end{aligned}
$$

It can be verified as usual that $n_2'' \equiv q_1^2q_2^2 + h\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \equiv A \pmod 3$, is invariant. We distinguish $A \equiv 0,\ 1,\ 2 \pmod 3$. If $A \equiv 0$ or $2 \pmod 3$, γ_{12} can always be so chosen that $n_1''' \equiv 0 \pmod 3$.

If $A \equiv 1 \pmod 3$, distinction must be made as to whether or not $n_1'' \equiv 0 \pmod 3$. If $n_1'' \equiv 0$, then $n_1''' \equiv 0 \pmod 3$, while if $n_1'' \not\equiv 0 \pmod 3$ we make, by a proper choice of ζ, $n_1''' \equiv 1 \pmod 3$.

The expression $A(A+1)n_1''$ is always $\equiv 0$ unless $A \equiv 1 \pmod 3$. In the latter case it is $\equiv 0 \pmod 3$ or not according as n_1'' is so or not. Put

$$B' \equiv A(A+1)h[(2q_1q_2^2+q_1)n_1+q_2n_2] \pmod 3.$$

It can be verified as usual that

$$B \equiv [B', 3] \pmod 3 \text{ is an invariant.*}$$

---

* Since B is perhaps the most difficult invariant to verify, I add the details of the verification. All other invariants which are not readily verified can be treated similarly. If we put $C \equiv h[(2q_1q_2^2+q_1)n_1+q_2n_2]$ (mod 3), and hence $B' \equiv A(A+1)C$ (mod 3), then B is invariant, and indeed congruent zero (mod 3), independently of C, when $A \equiv 0$, (mod 3); but when $A \equiv 1$, then $B' \equiv 2C$ (mod 3), and to show that $B \equiv [B', 3] \equiv [2C, 3]$ is invariant in this case also, it is necessary to show that in this case $[C, 3]$ is itself invariant.

We consider then the case that

$$A \equiv q_1^2q_2^2 + h \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \equiv 1 \pmod 3, \text{ and}$$

prove that for this value of A, $[C, 3]$ is invariant under the most general transformation admissible.

The most general transformation can be made up (Kronecker, Berl. Monatsberichte, 1866, Krazer, Annali di. Mat. Ser. 2, Vol. XII, Königsberger, Ell. Funkt., Vol. II, p. 70) out of the component transformations:

$$\begin{array}{lllll}
\text{I.} & \delta \equiv \delta, & \zeta \equiv 1, & |\gamma| \equiv \begin{vmatrix} 1, & 0 \\ 0, & 1 \end{vmatrix} & , \pmod 3, \\
\text{II.} & \delta \equiv 1, & \zeta \equiv \zeta, & |\gamma| \equiv \begin{vmatrix} 1, & 0 \\ 0, & 1 \end{vmatrix} & , (\text{ `` }), \\
\text{III.} & \delta \equiv 1, & \zeta \equiv 1, & |\gamma| \equiv \begin{vmatrix} 1, & 1 \\ 0, & 1 \end{vmatrix} & , (\text{ `` }), \\
\text{IV.} & \delta \equiv 1, & \zeta \equiv 1, & |\gamma| \equiv \begin{vmatrix} 0, & 1 \\ -1, & 0 \end{vmatrix} & , (\text{ `` }), \\
\text{V.} & \delta \equiv 1, & \zeta \equiv 1, & |\gamma| \equiv \begin{vmatrix} \gamma_{11}, & 0 \\ 0, & 1 \end{vmatrix} & , (\text{ `` }).
\end{array}$$

It appears easily that C is unaltered by transformations I and II. Applying transformation III, and denoting by C' the resulting expression, we have

$$C' \equiv h[\{2(q_1+q_2)q_2^2+q_1+q_2\}\{h(q_2-q_1)+n_1+n_2\}+q_2n_2] \pmod 3,$$

whence $\quad C' \equiv C + h(2q_1q_2^2+q_1)(hq_2-hq_1+n_2) \pmod 3.$

Put
$$\begin{aligned} D &\equiv h(2q_1q_2^2+q_1)(hq_2-hq_1+n_2) \quad (\text{ `` }), \\ &\equiv q_1(q_2^2-1)(q_1-hn_2) \quad (\text{ `` }). \end{aligned}$$

We have then as the result of this transformation $C' \equiv C + D$ (mod 3), and that C may be invariant under this transformation it is necessary and sufficient that $D \equiv 0$ (mod 3). D is evidently $\equiv 0$ (mod 3) if $q_1 \equiv 0$, or if $q_2 \not\equiv 0$ (mod 3), while if $q_1 \not\equiv 0$, $q_2 \equiv 0$ (mod 3),

$$D \equiv -q_1 - (q_1 - hn_2) \equiv -1 + hq_1n_2 \pmod 3.$$

But when $q_2 \equiv 0$ (mod 3) we have from $A \equiv 1$ (mod 3), $hq_1n_2 \equiv 1$ (mod 3) and hence $D \equiv 0$ (mod 3). C is therefore invariant under transformation III when $A \equiv 1$ (mod 3).

Applying transformation IV we have

$$C' \equiv C - hq_1q_2 \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \pmod 3.$$

Put
$$E \equiv hq_1q_2 \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \pmod 3.$$

Groups, Type $(1)(1)(11)$, $p=3$.

	1.)	2.)	3.)	4.)
$A\equiv 0$,		1,	1,	2,
$B\equiv 0$,		0,	1,	0.

49. *Case* $p=2$.

In this case, the generating relations are (cf. No. 44),

$$\begin{aligned} &a^2=1,\\ &b^2=a^m,\\ &\left.\begin{aligned} c_i^2&=a^{n_i}b^{f_i},\\ c_ib&=a^{q_i}bc_i,\end{aligned}\right\} i=1,\ 2,\\ &c_2c_1=a^tbc_1c_2,\\ &ab=ba,\\ &ac_i=c_ia,\ \ i=1,\ 2.\end{aligned}$$

Not both q_1 and q_2 may be congruent zero (mod 2), (No. 44).

Formulæ of multiplication (*cf. No.* 44):

$$c_i^\sigma b^\rho=a^{\sigma\rho q}b^\rho c_i^\sigma,\ \ i=1,\ 2,$$

$$c_2^\sigma c_1^\rho=a^{\sigma\rho\left[t+\frac{(\sigma-1)q_2+(\rho-1)q_1}{2}\right]}.\,b^{\rho\sigma}.\,c_1^\rho c_2^\sigma.$$

The following are the new relations consequent upon the given relations by transformation; transforming $c_1^2=a^{n_1}b^{f_1}$ by c_1 and by c_2, and also $c_2^2=a^{n_2}b^{f_2}$ by c_1 and by c_2, we reach respectively the following relations:

$$\begin{aligned} a^{f_1q_1}&=1,\\ a^{q_1+f_1q_2+m}&=1,\\ a^{q_2+f_2q_1+m}&=1,\\ a^{f_2q_2}&=1.\end{aligned}$$

That C may be invariant when $A\equiv 1$ (mod 3) we must have then $E\equiv 0$ (mod 3). This is evidently the case if q_1 or $q_2\equiv 0$ (mod 3), while if $q_1\not\equiv 0$, $q_2\not\equiv 0$ (mod 3), we have from $A\equiv 1$, $1+h\begin{vmatrix} q_1, & q_2\\ n_1, & n_2\end{vmatrix}\equiv 1$, (mod 3), whence $\begin{vmatrix} q_1, & q_2\\ n_1, & n_2\end{vmatrix}\equiv 0$ (mod 3), or $E\equiv 0$ (mod 3). Therefore when $A\equiv 1$ (mod 3), C is invariant under transformation IV.

Applying transformation V, we find readily that $C'\equiv\gamma_{11}C$ (mod 3). Since $\gamma_{11}\not\equiv 0$ (mod 3), $[C, 3]$ is invariant under this transformation.

We have now shown that $[C, 3]$ is invariant when $A\equiv 1$, (mod 3), and that, consequently, $B\equiv[B', 3]\equiv[A(A+1)C, 3]$ (mod 3) is an invariant of the type.

Whence (note No. 20),

$$\begin{aligned} q_2 + f_2 q_1 + m &\equiv 0 \pmod 2, \\ q_1 + f_1 q_2 + m &\equiv 0 \ (\ \text{"}\ ), \\ f_1 q_1 &\equiv 0 \ (\ \text{"}\ ), \\ f_2 q_2 &\equiv 0 \ (\ \text{"}\ ). \end{aligned}$$

From these congruences it appears that

$$\begin{aligned} m &\equiv 1 \qquad \pmod 2, \\ f_1 &\equiv 1 + q_1 \ (\ \text{"}\ ), \\ f_2 &\equiv 1 + q_2 \ (\ \text{"}\ ). \end{aligned}$$

Making the following most general choice of generating elements (cf. No. 46),

$$\begin{aligned} a' &= a, \\ b' &= a^{\epsilon} b, \\ c_i' &= b^{\beta_i} c_1^{\gamma_{i1}} c_2^{\gamma_{i2}}, \quad i = 1,\ 2, \quad |\gamma| \not\equiv 0 \pmod 2, \end{aligned}$$

and denoting by $G\left[\frac{N}{2}\right]$ the greatest integer in $\frac{N}{2}$ if $\frac{N}{2}$ is positive or zero, and one more than the greatest integer in $\frac{N}{2}$ taken with the positive sign if $\frac{N}{2}$ is negative; and by $R[N]$ the smallest non-negative remainder of N (mod 2), we find as usual the following

Formulæ of transformation:

$$\begin{aligned} f_i' &= R[\gamma_{i1}\gamma_{i2} + f_1\gamma_{i1} + f_2\gamma_{i2}]^*, \quad i = 1,\ 2, \\ n_i' &\equiv \gamma_{i1}\gamma_{i2}\left[t + \frac{(\gamma_{i1} - 1)q_1 + (\gamma_{i2} - 1)q_2}{2} + \gamma_{i1} q_1\right] \\ &\quad + \beta_i[1 + \gamma_{i1} q_1 + \gamma_{i2} q_2] + \gamma_{i1} n_1 + \gamma_{i2} n_2 \\ &\quad + G\left[\frac{\gamma_{i1}\gamma_{i2} + f_1\gamma_{i1} + f_2\gamma_{i2}}{2}\right] \\ &\quad + \varepsilon R[\gamma_{i1}\gamma_{i2} + f_1\gamma_{i1} + f_2\gamma_{i2}], \pmod 2, \quad i = 1,\ 2, \\ q_i' &\equiv \gamma_{i1} q_1 + \gamma_{i2}, \pmod 2, \quad i = 1,\ 2, \\ t' &\equiv t + \Big\{ \beta_1\gamma_{21} + \beta_2\gamma_{11} + \gamma_{11}\gamma_{21}(\gamma_{22} - \gamma_{12}) \\ &\quad + \frac{\gamma_{11}\gamma_{22}(\gamma_{11} - 1) - \gamma_{12}\gamma_{21}(\gamma_{21} - 1)}{2} \Big\} q_1 \\ &\quad + \left\{ \beta_1\gamma_{22} + \beta_2\gamma_{11} + \frac{\gamma_{11}\gamma_{22}(\gamma_{22} - 1) - \gamma_{12}\gamma_{21}(\gamma_{12} - 1)}{2} \right\} q_2 \\ &\quad + \varepsilon + G\left[\frac{1 - |\gamma|}{2}\right], \pmod 2. \end{aligned}$$

---

* It is to be noticed particularly that, since $b^2 = a$, the exponents of b in the relations may not be altered by arbitrary multiples of 2, and that the quantities f must therefore be supposed to have their smallest non-negative values (mod 2), and that f_i' must be taken *equal* to the expression given.

We now apply a transformation to make the q's both unity, viz.

$$|\gamma| \equiv \begin{vmatrix} q_1, & q_1 + q_2 \\ q_1 + q_2, & q_2 \end{vmatrix}, \ \beta_i \equiv 0, \ \varepsilon \equiv 0, \ (\text{mod } 2),$$

and remembering that $\alpha^2 \equiv \alpha$, and $q_1 + q_2 + q_1 q_2 \equiv 1$ (mod 2), and supposing the smallest non-negative values of the q's (mod 2) to have been taken originally, we have the results:

$$\begin{aligned} n_1' &\equiv (1 + q_2)t + q_1 n_1 + (q_1 + q_2) n_2, \ (\text{mod } 2), \\ n_2' &\equiv (1 + q_1)t + 1 + q_1 + (q_1 + q_2) n_1 + q_2 n_2, \ (\text{mod } 2), \\ q_1' &= 1; \ f_1' = 0, \\ q_2' &= 1; \ f_2' = 0. \end{aligned}$$

The most general transformation which will leave these values of q_1, q_2 unaltered is

$$|\gamma| \equiv \begin{vmatrix} \gamma_{11}, & 1 - \gamma_{11} \\ 1 - \gamma_{11}, & \gamma_{11} \end{vmatrix} \ (\text{mod } 2), \ \beta_i, \ \varepsilon \text{ arbitrary.}$$

Neither ε nor β_i has any effect upon the n's when $q_1 \equiv q_2 \equiv 1$, (mod 2). By giving ε a proper value we make $t'' \equiv 0$ (mod 2). The resulting values of $n_1 n_2$ are,

$$\begin{aligned} n_1'' &\equiv \gamma_{11} n_1' + (1 - \gamma_{11}) n_2' \ (\text{mod } 2), \\ n_2'' &\equiv (1 - \gamma_{11}) n_1' + \gamma_{11} n_2' \ (\ \text{``}\ ). \end{aligned}$$

Adding and multiplying these values, we have respectively,

$$\begin{aligned} n_1'' + n_2'' &\equiv n_1' + n_2', \ (\text{mod } 2), \\ n_1'' n_2'' &\equiv n_1' n_2', \quad (\ \text{``}\ ). \end{aligned}$$

Written in terms of the original parameters, these are then two invariants, viz.

$$\begin{aligned} A &\equiv n_1' + n_2' \equiv (q_1 + q_2)t + q_1 + 1 + q_2 n_1 + q_1 n_2 \ (\text{mod } 2), \\ B &\equiv n_1' n_2' \equiv (1 + q_2)t n_1 + (1 + q_1)t n_2 + (1 + q_2) n_1 + n_1 n_2 \ (\text{mod } 2). \end{aligned}$$

Since we have reduced all the other parameters to a single set of values, irrespective of the n's, the invariants A and B distinguish completely the groups.

Groups, Type $(1)(1)(11)$, $p = 2$.

	1.)	2.)	3.)
$A \equiv$	0,	1,	0,
$B \equiv$	0,	0,	1.

50. *Summary of results.*

In the following summary of results there are given first, the generating relations of each type in their general form, then the invariants, and last, all the existent groups, except the commutative groups, defined as well by values of the invariants, as by generating relations in which the exponents form a set of "reduced" values (No. 25).

GROUPS OF ORDER p^3.

Type (1)(11).

Relations:

$$a^p = 1,$$
$$b_i^p = a^{m_i}, \quad i = 1, 2,$$
$$b_2 b_1 = a^n b_1 b_2,$$
$$a b_i = b_i a, \quad i = 1, 2.$$

Case $p > 2$.

Invariant: $A = [m_1, m_2, p]$.

Groups: $A = 1, p$.

	1).	2).
$a^p =$	1	1
$b_1^p =$	a	1
$b_2^p =$	1	1

$$\left.\begin{aligned} b_2 b_1 &= a b_1 b_2, \\ a b_i &= b_i a, \end{aligned}\right\} \text{in both groups.}$$

Case $p = 2$.

Invariant: $A \equiv m_1 m_2 \pmod 2$.

Groups: $A \equiv 1, 0 \pmod 2$.

	1).	2).
$a^2 =$	1	1
$b_1^2 =$	a	1
$b_2^2 =$	a	1

$$\left.\begin{aligned} b_2 b_1 &= a b_1 b_2, \\ a b_i &= b_i a, \end{aligned}\right\} \text{in both groups.}$$

GROUPS OF ORDER p^4.

Type (2)(11).

Relations:

$$a^{p^2} = 1,$$
$$b_i^p = a^{m_i}, \quad i = 1, 2,$$
$$b_2 b_1 = a^n b_1 b_2,$$
$$a b_i = b_i a, \quad i = 1, 2.$$

Invariant: $A = [m_1, m_2, p]$.

Groups: $A = p, 1$.

	1).	2).
$a^{p^2} =$	1	1
$b_1^p =$	1	a
$b_2^p =$	1	1

$$\left.\begin{aligned} b_2b_1 &= a^pb_1b_2, \\ ab_i &= b_ia, \quad i = 1, 2, \end{aligned}\right\} \text{in both groups.}$$

Type $(11\chi 11)$.

Relations:

$$\left.\begin{aligned} a_i^p &= 1, \\ b_i^p &= a_1^{m_{i1}}a_2^{m_{i2}}, \end{aligned}\right\} i, = 1, 2,$$

$$b_2b_1 = a_1^{n_1}a_2^{n_2}b_1b_2,$$

$$a_2a_1 = a_1a_2,$$

$$a_ib_j = b_ja_i, \quad i, j = 1, 2, \text{ independently.}$$

e $p > 2$.

riants:

$$A = [|m|, p],$$

$$B = \left[\begin{vmatrix} n_1, & m_{11}, \\ n_2, & m_{12}, \end{vmatrix}, \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix}, p\right],$$

$$C = [m_{11}, m_{12}, m_{21}, m_{22}, p].$$

Groups:

	1).	2).	3).	4).
$A =$	1	p	p	p
$B =$	1	1	p	p
$C =$	1	1	1	p
$a_1^p =$	1	1	1	1
$a_2^p =$	1	1	1	1
$b_1^p =$	a_1	1	1	1
$b_2^p =$	a_2	a_2	a_1	1

$$\left.\begin{aligned} b_2b_1 &= a_1b_1b_2, \\ a_ib_j &= b_ja_i, \quad i, j = 1, 2 \\ a_2a_1 &= a_1a_2 \end{aligned}\right\} \text{in all these groups.}$$

Case $p = 2$.

Invariants:

$$A \equiv \left[\begin{vmatrix} n_1, & m_{11} \\ n_2, & m_{12} \end{vmatrix}, \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix}, 2 \right], \text{ (mod 2)},$$

$$B \equiv \begin{vmatrix} m_{11}, & n_1 + n_2 \\ m_{12}, & n_1 \end{vmatrix} \cdot \begin{vmatrix} m_{21}, & n_1 + n_2 \\ m_{22}, & n_1 \end{vmatrix} \cdot (A + 1), \text{ (mod 2)},$$

$$C \equiv \begin{vmatrix} n_1, & m_{11} \\ n_2, & m_{12} \end{vmatrix} \begin{vmatrix} n_1, & m_{21} \\ n_2, & m_{22} \end{vmatrix} + \begin{vmatrix} m_{11}, & m_{12} \\ m_{21}, & m_{22} \end{vmatrix}, \text{ (mod 2)}.$$

Groups:

	1).	2).	3).	4).
$A \equiv$	0	1	1	0
$B \equiv$	1	0	0	0
$C \equiv$	0	1	0	0
$a_1^2 =$	1	1	1	1
$a_2^2 =$	1	1	1	1
$b_1^2 =$	a_1	a_1	1	1
$b_2^2 =$	a_1	a_2	a_2	1

$$\left.\begin{aligned} b_2 b_1 &= a_1 b_1 b_2, \\ a_i b_j &= b_j a_i, \quad i, j = 1, 2, \\ a_1 a_2 &= a_2, a_1, \end{aligned}\right\} \text{in all these groups.}$$

Type (1)(1)(11).

Relations:

$$\begin{aligned} a^p &= 1, \\ b^p &= a^m, \\ \left.\begin{aligned} c_i^p &= a^{n_i} b^{f_i}, \\ c_i b &= a^{q_i} b c_i, \end{aligned}\right\} & \; i = 1, 2, \\ c_2 c_1 &= a^t b^h c_1 c_2, \\ ab &= ba, \\ ac_i &= c_i a, \quad i = 1, 2. \end{aligned}$$

Case $p > 3$.

Invariants: $A \equiv [n_1, n_2, p]$, (mod p),

$$B \equiv \left[\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}, p \right], \text{ (mod } p\text{)},$$

$$C = \left(\frac{\begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix}}{p} \right).$$

Groups:

	1).	2).	3).	4).
$A \equiv$	0	1	1	1
$B \equiv$	0	0	1	1
$C =$	$+1$	$+1$	$+1$	-1
$a^p =$	1	1	1	1
$b^p =$	1	1	1	1
$c_1^p =$	1	a	1	1
$c_2^p =$	1	1	a	a^N

(N any quadratic non-residue of p),

$$\left.\begin{array}{l} c_1 b = abc_1, \\ c_2 b = bc_2, \\ c_2 c_1 = bc_1c_2, \\ ab = ba, \\ ac_i = c_i a, \quad i = 1,\ 2 \end{array}\right\} \text{ in all these groups.}$$

Case $p = 3$.

Invariants: $A \equiv q_1^2 q_2^2 + h \begin{vmatrix} q_1, & q_2 \\ n_1, & n_2 \end{vmatrix} \pmod 3$,

$$B \equiv [A(A+1)h\{(2q_1q_2^2 + q_1)n_1 + q_2n_2\},\ 3] \pmod 3.$$

Groups:

	1).	2).	3).	4).
$A \equiv$	0	1	1	2
$B \equiv$	0	0	1	0
$a^3 =$	1	1	1	1
$b^3 =$	1	1	1	1
$c_1^3 =$	1	1	a	1
$c_2^3 =$	1	a	a	a^2

$$\left.\begin{array}{l} c_1 b = abc_1, \\ c_2 b = bc_2, \\ c_2 c_1 = bc_1c_2, \\ ab = ba, \\ ac_i = c_i a. \end{array}\right\} \text{ in all these groups.}$$

Case $p = 2$.

Invariants:

$$A \equiv (q_1 + q_2)t + q_1 + 1 + q_2n_1 + q_1n_2 \pmod 2,$$

$$B \equiv (1 + q_2)tn_1 + (1 + q_1)tn_2 + (1 + q_2)n_1 + n_1n_2 \pmod 2.$$

Groups:

	1).	2).	3).
$A \equiv$	0	1	0
$B \equiv$	0	0	1
$a^2 =$	1	1	1
$b^2 =$	a	a	a
$c_1^2 =$	1	a	a
$c_2^2 =$	1	1	a

$$\left.\begin{aligned} c_i b &= abc_i, \quad i = 1,\ 2, \\ c_2 c_1 &= bc_1 c_2, \\ ab &= ba, \\ ac_i &= c_i a, \quad i = 1,\ 2, \end{aligned}\right\} \text{ in all these groups.}$$

§3.

51. *Groups of order* 16.

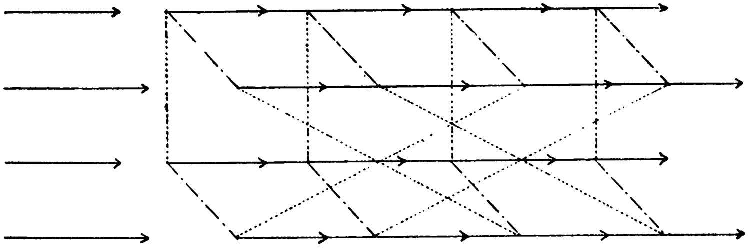
I add a table of the "color groups,"* presenting graphically, in Cayley's method, the non-commutative groups of order 16 as regular transitive groups of substitutions operating on sixteen letters.

Each group can be generated by three, or fewer, elements properly chosen. To these we shall assign the colors red, green and black, and shall denote them by the letters R, G, B, and in the figures by the lines ————, ..., —·—·—·—·—·—, respectively. We shall give, for each group, the new generating elements expressed in terms of those of the preceding paragraph, then the relations which the new generating elements satisfy, and last, the color-diagrams.

Type (2)(11).

Group 1).

$$\begin{aligned} R &= a, & R^4 &= 1, & RB &= BR, \\ B &= b_1, & B^2 &= 1, & RG &= GR, \\ G &= b_2, & G^2 &= 1, & GB &= R^2 BG. \end{aligned}$$

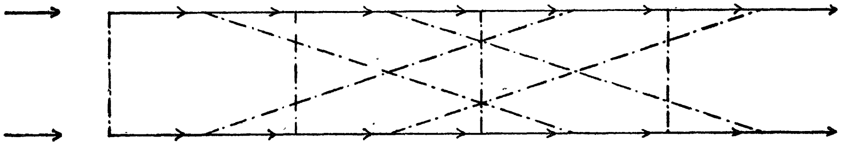


---

* Cayley, Am. J. Math., Vol. XI, p. 139.

Group 2).

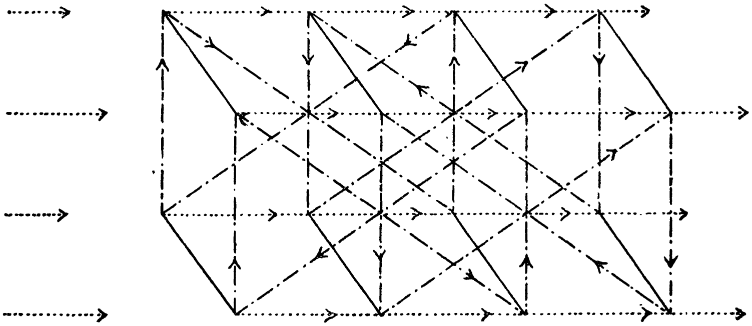
$$R = b_1, \quad R^8 = 1,$$
$$B = b_2, \quad B^2 = 1, \quad BR = R^5 B.$$



Type (11)(11).

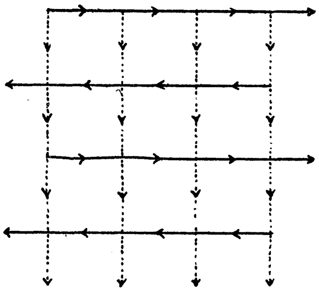
Group 1).

$$R = a_2, \quad G^4 = 1, \quad G^2 = B^2,$$
$$G = b_1, \quad B^4 = 1, \quad BG = G^3 B,$$
$$B = b_2, \quad R^2 = 1, \quad RG = GR, \quad RB = BR.$$



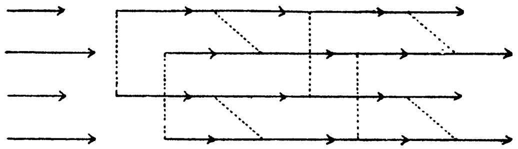
Group 2).

$$R = b_1, \quad R^4 = 1,$$
$$G = b_2, \quad G^4 = 1, \quad GR = R^3 G.$$



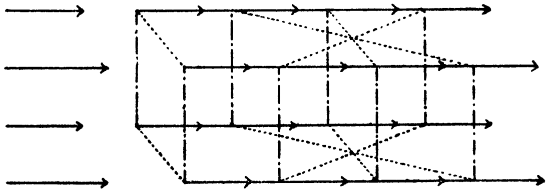
Group 3).

$$R = b_2 b_1, \quad R^4 = 1,$$
$$G = b_1, \quad G^2 = 1, \quad R^2 G = G R^2.$$



Group 4).

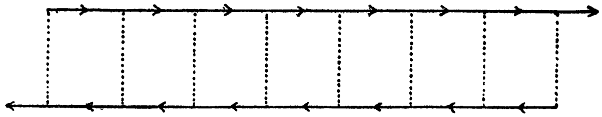
$$B = a_2, \quad R^4 = 1, \quad GB = BG,$$
$$R = b_2 b_1, \quad B^2 = 1, \quad RB = BR,$$
$$G = b_1, \quad G^2 = 1, \quad GR = R^3 G.$$



Type (1)(1)(11).

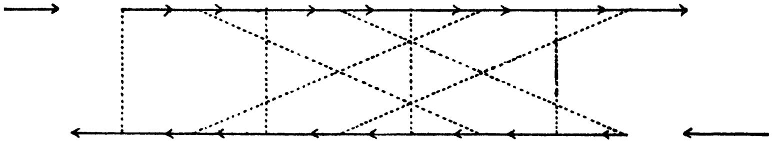
Group 1).

$$R = c_2 c_1, \quad R^8 = 1,$$
$$G = c_2, \quad G^2 = 1, \quad RG = GR^7.$$



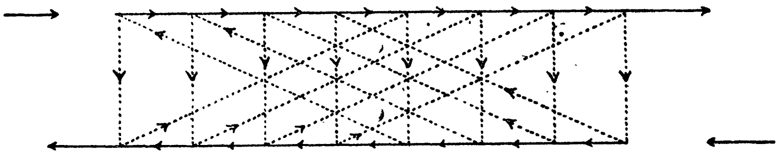
Group 2).

$$R = c_2 c_1, \quad R^8 = 1,$$
$$G = c_2, \quad G^2 = 1, \quad RG = GR^3.$$



Group 3).

$$R = c_2 c_1, \quad R^8 = 1, \quad G^2 = R^4,$$
$$G = c_2, \quad G^4 = 1, \quad GR = R^7 G.$$



52. It is of interest to compare with these results the various particular groups of order 16 already known. I shall mention here only the most important groups of order 16 previously given, viz. those contained in Cayley's list of groups of substitutions on eight letters.* To determine whether or not a given group of order 16 is expressible as a group of substitutions on eight letters, and if so, to find the group of substitutions, we use the method given by Dyck.† It is, in brief, this:

If a group G, of order $N = \mu . \nu$, contains a subgroup of order μ, the elements of G can be distributed into the following "systems of imprimitivity":

$$1, A_2, \ldots . A_\mu \,|\, B_2, A_2 B_2, \ldots . A_\mu B_2 \,|\, \ldots\ldots\ldots\ldots \,|\, B_\nu, A_2 B_\nu, \ldots . A_\mu B_\nu .$$

Call these systems respectively $C_1, C_2, \ldots . C_\nu$. By the definition of imprimitivity it follows that when the elements of the group G are multiplied throughout by any element of G, there results a substitution on $C_1, C_2, \ldots . C_\nu$. Multiplying the elements of G successively by its N elements, there result N substitutions on $C_1, C_2, \ldots . C_\nu$, forming a group G'. Some of these substitutions may however be identical. Dyck shows that the necessary and sufficient condition that the group G' (of substitutions on ν letters) be actually of order N and holoedrically isomorphic with the group G, (identical with G in the sense of this paper), is that the subgroup $1, A_2, \ldots . A_\mu$, used in the determination of G', shall neither be a self-conjugate subgroup of G nor contain any self-conjugate subgroup of G.

In our case, $N = 16$, $\nu = 8$, $\mu = 2$, and every subgroup of order 2, not a self-conjugate subgroup of G, leads to a group of order 16 of substitutions on eight letters. Making examination in this way of the non-commutative groups of order 16 enumerated above, we find that the following of them can be expressed as transitive groups of substitutions on eight letters:

---

* Quar. J. Math. No. 98, 1891, p. 137.

† Math. Annalen, Vol. XXII, p. 90.

Group.	*Number in Cayley's list.*[*]
(2)(11), 1),	20,
2),	23,
(11)(11), 3),	22,
4),	21,
(1)(1)(11), 1),	v. below,
2),	“

The group (1)(1)(11), 1), expressed as a transitive group of substitutions operating on eight letters, is generated by the substitutions

$$(bh)(cg)(df)$$

and

$$(abcdefgh),$$

while the group (1)(1)(11), 2), similarly expressed, is generated by the substitutions

$$(bd)(cg)(fh)$$

and

$$(abcdefgh).$$

I have not been able to identify these two groups with any of the groups of Cayley's list.

§4.

53. *Type* $(\kappa)(11\ldots.1)$, s units in the second parenthesis.

The groups of this type are generated by elements a, b_i, $(i = 1, 2, \ldots. s,)$ satisfying the relations:

$$\begin{array}{ll} a^{p^\kappa} = 1, & \\ b_i^h = a^{m_i} & i = 1, 2, \ldots. s \\ b_jb_i = a^{n_{ij}}b_ib_j, & i, j = 1, 2\ldots. s, \text{ independently}, \\ ab_i = b_ia, & i = 1, 2\ldots. s. \end{array}$$

From the third relation we have

$$n_{ij} \equiv -n_{ji},\ n_{ii} \equiv 0,\ (\text{mod } p^\kappa).$$

---

[*] Quar. J. Math. 1891, p. 140.

Formulæ of multiplication:

$$b_j^{\beta_j} b_i^{\beta_i} = a^{\beta_j \beta_i n_{ij}} b_i^{\beta_i} b_j^{\beta_j},$$

$$(a^{\alpha} b_1^{\beta_1} b_2^{\beta_2} \dots b_s^{\beta_s})^q = a^{q\alpha + \frac{q(q-1)}{2} \sum\limits_{j=i+1}^{s} \sum\limits_{i=1}^{s-1} \beta_i \beta_j n_{ij}} b_1^{q\beta_1} b_2^{q\beta_2} \dots b_s^{q\beta_s},$$

$$b_1^{\beta_{l1}} b_2^{\beta_{l2}} \dots b_s^{\beta_{ls}} . b_1^{\beta_{\kappa 1}} b_2^{\beta_{\kappa 2}} \dots b_s^{\beta_{\kappa s}} = a^{\sum\limits_{j=i+1}^{s} \sum\limits_{i=1}^{s-1} \beta_{\kappa i} \beta_{lj} n_{ij}} b_1^{\beta_{l1} + \beta_{\kappa 1}} b_2^{\beta_{l2} + \beta_{\kappa 2}} \dots b_s^{\beta_{ls} + \beta_{\kappa s}},$$

$$b_1^{\beta_{l1}} b_2^{\beta_{l2}} \dots b_s^{\beta_{ls}} . b_s^{\beta_{hs}} b_{s-1}^{\beta_{h,s-1}} \dots b_2^{\beta_{h2}} b_1^{\beta_{h1}} = a^{\sum\limits_{j=\kappa+1}^{s} \sum\limits_{\kappa=1}^{s-1} (\beta_{lj} + \beta_{hj}) \beta_{h\kappa} n_{\kappa j}} . b_1^{\beta_{h1} + \beta_{l1}} b_2^{\beta_{h2} + \beta_{l2}} \dots b_s^{\beta_{hs} + \beta_{ls}},$$

$$b_s^{\beta_{is}} b_{s-1}^{\beta_{i,s-1}} \dots b_2^{\beta_{i2}} b_1^{\beta_{i1}} . b_1^{\beta_{j1}} b_2^{\beta_{j2}} \dots b_s^{\beta_{js}} = a^{\sum\limits_{\kappa=l+1}^{s} \sum\limits_{l=1}^{s-1} \beta_{i\kappa} (\beta_{jl} + \beta_{il}) n_{l\kappa}} . b_1^{\beta_{j1} + \beta_{i1}} b_2^{\beta_{j2} + \beta_{i2}} \dots b_s^{\beta_{js} + \beta_{is}}.$$

By transforming the second relation given by b_j we find that

$$a^{pn_{ij}} b_i^p = a^{m_i}, \text{ and hence}$$
$$a^{pn_{ij}} = 1.$$

From this it follows (v. note to No. 20) that $p_{n_{ij}} \equiv 0 \pmod{p^{\kappa}}$ or $n_{ij} \equiv 0 \pmod{p^{\kappa-1}}$ for all values of i and j. This restriction upon the n's is necessary in order that the group generated by the elements satisfying the relations given may be of the type in question. Supposing the n's chosen subject to this restriction, no new relations arise from transforming all of the generating relations by each of the generating elements, and the only consequences of the given relations are, therefore, their products and powers.

54. We next determine the condition that no element other than a and its powers be commutative with every element of the group. Suppose

$$g = a^{\alpha} b_1^{\gamma_1} \dots b_s^{\gamma_s}$$

were commutative with every element of the group. To this end it is necessary and sufficient that g be commutative severally with $b_1, b_2, \dots b_s$. For g is certainly commutative with a, and every element of the group can be expressed as a product of a and b_i's. I. e., that g be commutative with every element of the group it is necessary and sufficient that

$$g b_l = b_l g,$$

or

$$a^{\alpha} b_1^{\gamma_1} \dots b_s^{\gamma_s} b_l = b_l . a^{\alpha} b_1^{\gamma_1} \dots b_s^{\gamma_s}, \quad l = 1, 2 \dots s.$$

Whence, reducing and applying multiplication formulæ,

$$a^{\sum\limits_{j=l+1}^{s} \gamma_l n_{lj}} = a^{\sum\limits_{j=1}^{l-1} \gamma_j n_{lj}}, \quad l = 1, 2 \dots s.$$

From this,

$$\sum_{j=l+1}^{s} \gamma_j n_{lj} \equiv \sum_{j=1}^{l-1} \gamma_j n_{jl}, \text{ (mod. } p^{\kappa}), \quad l = 1, 2 \ldots . s,$$

or since $n_{lj} \equiv - n_{jl}$, $n_{jj} \equiv 0$, (mod p^{κ}),

$$\sum_{j=1}^{s} \gamma_j n_{jl} \equiv 0 \text{ (mod } p^{\kappa}), \quad l = 1, 2, \ldots . s.$$

Every set of γ's satisfying this system of s congruences determines an element $a^{\alpha} b_1^{\gamma_1} b_2^{\gamma_2} \ldots . b_s^{\gamma_s}$, which is commutative with every element of the group. But, by hypothesis, no elements other than powers of a are commutative with every element of the group; hence the only admissible values of γ are $\gamma_j \equiv 0$ (mod p), $j = 1, 2, \ldots . s$. The n's must, therefore, be further restricted to such values that the system of congruences above can be satisfied only by $\gamma_j \equiv 0$ (mod p), $j = 1, 2, \ldots . s$.

55. Frobenius* has shown that there is a one-to-one correspondence between the system of congruences under consideration and those of the system

$$\sigma_j \gamma_j' \equiv 0 \text{ (mod } p^{\kappa}), \quad j = 1, 2, \ldots . s,$$

where σ_j is a quantity defined as follows: Given a square array of m^2 integers. Let d_λ be the positive greatest common divisor of all the determinants of order λ that can be formed by striking out $m - \lambda$ rows and $m - \lambda$ columns of this array. In case the value of every determinant of order λ should be zero, d_λ is taken to be zero also. Since every determinant of order λ is a linear homogeneous function of determinants of order $\lambda - 1$, $e_\lambda = \dfrac{d_\lambda}{d_{\lambda-1}}$ is also an integer. $\Big($We fix that $e_1 = d_1$, and if $e_\mu = \dfrac{0}{0}$, then $e_\mu = 0$.$\Big)$ The integer e_λ, so defined, is called the λ^{th} *elementary divisor* of the given array, and σ_λ is defined by the following equation:

$$\sigma_\lambda = [e_\lambda, p^{\kappa}].$$

Frobenius shows† that $\dfrac{\sigma_\lambda}{\sigma_{\lambda-1}}$ is also an integer.

---

* Crelle's Journal, Vol. 86, pp. 191-2. See also Smith, Phil. Trans. 1861, p. 293. The notation used above is that of Frobenius.

† *Loc. cit.*, pp. 189-90.

That the congruences

$$\sum_{j=1}^{s} \gamma_j n_{jl} \equiv 0 \pmod{p^\kappa}, \quad l = 1, 2, \ldots . s,$$

be satisfied only by $\gamma_j \equiv 0 \pmod{p^\kappa}$, $j = 1, 2, \ldots . s$, it is necessary and sufficient that the congruences

$$\sigma_j \gamma_j' \equiv 0 \pmod{p^\kappa}, \quad j = 1, 2, \ldots . s$$

(σ_j being now defined by the array of integers n_{ij}), be satisfied only by

$$\gamma_j' \equiv 0 \pmod{p}, \quad j = 1, 2, \ldots . s.$$

And to this end it is necessary and sufficient that $\sigma_j \not\equiv 0 \pmod{p^\kappa}$, $j = 1, 2, \ldots . s$, or, since $\frac{\sigma_\lambda}{\sigma_{\lambda-1}}$ is an integer, that

$$\sigma_s \not\equiv 0 \pmod{p^\kappa}.$$

But

$$\sigma_s = [e_s, p^\kappa] = \left[\frac{d_s}{d_{s-1}}, p^\kappa\right] = \left[\frac{|n|}{d_{s-1}}, p^\kappa\right].$$

Hence, that $\sigma_s \not\equiv 0 \pmod{p^\kappa}$ it is necessary that $|n|$ be not *absolutely* zero in value, although the congruence $|n| \equiv 0 \pmod{p^\kappa}$ may hold. This, then, is the condition that no element but a and its powers be commutative with every element of the group.

Further, $|n|$ is a skew symmetric determinant, and not being zero, it must be of *even* order, $s = 2\rho$.* Hence follows the theorem:

The last parenthesis in the type symbol must always contain an even number of integers.

56. We make now the most general choice of generating elements, a', b_i', for the group G, viz:

$$a' = a^\delta,$$
$$b_i' = a_1^{\alpha_i} b_2^{\beta_{i1}} b_1^{\beta_{i2}} \ldots . b_s^{\beta_{is}}, \quad i = 1, 2, \ldots . s, \quad s = 2\rho.$$

By the methods already explained (Nos. 22, 23), it appears that the necessary and sufficient conditions that the elements a', b_i' generate the group G itself are

$$\delta \not\equiv 0, \quad |\beta| \not\equiv 0 \pmod{p},$$

α_i being arbitrary.

---

* Baltzer, Determinanten, §§5, 8.

The cases $p > 2$ and $p = 2$ must now be distinguished.

Formulæ of Transformation, $p > 2$.

$$\delta\left(p\alpha_i + \sum_{j=1}^{s}\beta_{ij}m_j\right) \equiv m_i' \pmod{p^\kappa}, \quad i = 1, 2, \ldots . s,$$

$$\delta\sum_{h=1}^{s}\sum_{l=1}^{s}\beta_{il}\beta_{jh}n_{lh} \equiv n_{ij}' \pmod{p^\kappa}, \quad \begin{matrix} i = 1, 2, \ldots . s - 1, \\ j = i + 1, \ldots . s. \end{matrix}$$

It appears from the form of the expression for m_i', together with the fact that the m's are expressible in terms of the m's by like formulæ, that

$$A = [m_1, m_2, \ldots . m_s, p]$$

is an invariant.

Frobenius* has shown that a system of integers β_{ij}, of determinant unity, can be chosen such that

$$\left.\begin{matrix} n_{i,\,\rho+i}' \equiv \sigma_{2i} \pmod{p^\kappa} \\ n_{\rho+i,\,i}' \equiv -\,\sigma_{2i} \pmod{p^\kappa} \end{matrix}\right\} i = 1, 2, \ldots . \rho,$$
$$n_{ij}' \equiv 0 \pmod{p^\kappa} \text{ for all other values of } i \text{ and } j.$$

In view of the restrictions upon the integers n_{ij} already found, we have $e_1 = rp^{\kappa-1}$, $r \not\equiv 0 \pmod{p}$, $\sigma_1 = p^{\kappa-1}$. Since $\frac{\sigma_\lambda}{\sigma_{\lambda-1}}$ is an integer and $\sigma_{2\rho} \not\equiv 0 \pmod{p^\kappa}$, $\sigma_j = p^{\kappa-1}$ for all values of j.

We have, then,

$$n_{i,\,\rho+1}' \equiv -\,n_{\rho+i,\,i} \equiv p^{\kappa-1} \pmod{p^\kappa}, \; i = 1, 2, \ldots . \rho,$$
$$n_{ij}' \equiv 0 \pmod{p^\kappa} \text{ for all other values of } i \text{ and } j.$$

We apply now the most general transformation, leaving the n''s unaltered. To this end the β's and δ must be so chosen that

$$\delta\sum_{h=1}^{s}\sum_{l=1}^{s}\beta_{il}\beta_{jh}n_{lh}' \equiv n_{ij}' \pmod{p^\kappa} \quad \begin{matrix} i = 1, 2, \ldots . s - 1, \\ j = i + 1, \ldots . s, \end{matrix}$$

---

*Crelle's Journal, Vol. 86, pp. 146–191; in particular, pp. 165–168, 187–191. There is a slight difference in form between the result given above and Frobenius' result. If, in the bilinear form $\sum_{\alpha,\beta} n_{\alpha\beta}x_\alpha y_\beta$, used by Frobenius, $y_{2\kappa}$, $x_{2\kappa}$, $y_{2\kappa-1}$, $x_{2\kappa-1}$, be replaced respectively by $y_{\rho+\kappa}$, $x_{\rho+\kappa}$, y_κ, x_κ, the result is reached in the form above.

or, substituting the values of n', that

$$\begin{aligned}\bar{\delta}\sum_{l=1}^{\rho}(\beta_{il}\beta_{j,\,\rho+l}-\beta_{i,\,\rho+l}\beta_{jl})\,p^{\kappa-1} &\equiv p^{\kappa-1} \pmod{p^{\kappa}} \text{ if } i=j-\rho,\\ &\equiv -p^{\kappa-1} \pmod{p^{\kappa}} \text{ if } i=j+\rho,\\ &\equiv 0 \pmod{p^{\kappa}} \text{ in all other cases,}\end{aligned}$$

i. e., that*

$$\begin{aligned}\sum_{l=1}^{\rho}(\beta_{il}\beta_{j,\,\rho+l}-\beta_{i,\,\rho+l},\ \beta_{jl}) &\equiv \delta \pmod{p}, \text{ if } i=j-\rho,\\ &\equiv -\delta \pmod{p}, \text{ if } i=j+\rho,\\ &\equiv 0 \pmod{p} \text{ in all other cases.}\end{aligned}$$

57. We have already found an invariant A. When $A=p$, then

$$m_i\equiv 0 \pmod{p},\ i=1,\ 2,\ \ldots .\ s.$$

In this case it is always possible, by a proper choice of α_i, to make

$$m_i\equiv 0 \pmod{p^{\kappa}},\ i=1,\ 2,\ \ldots .\ s.$$

All the sets of values of m_i for which $A=p$ are then reducible to the set just written; i. e., there is only one group for which $A=p$.

In case $A=1$, it is possible by a proper choice of α_i always to make $0\leqq m_i<p$. We suppose this done. The following are particular sets of values of δ, β_{ij}, which satisfy the conditions at the end of No. 56:

$$|\beta|\equiv\left|\begin{array}{l|l}
1\quad 0\ \cdots\cdots\cdots\ 0 & 0\ \cdots\ 0\ \cdots\ 0\\
0\quad 1\ \cdots\cdots\cdots\ 0 & \cdots\cdots\cdots\cdots\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
0\quad 0\ \cdots\ \beta_{ii}\ \cdots\ 0 & 0\ \cdots\ \beta_{i,\,\rho+i}\ \cdots\ 0\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
0\quad 0\ \cdots\cdots\cdots\ 1 & 0\ \cdots\ 0\ \cdots\ 0\\
\hline
0\quad 0\ \cdots\cdots\cdots\ 0 & 1\quad 0\ \cdots\ 0\ \cdots\ 0\\
\cdots\cdots\cdots\cdots & 0\quad 1\ \cdots\ 0\ \cdots\ 0\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
0\quad 0\ \cdots\ \beta_{\rho+i,\,i}\ \cdots\ 0 & 0\quad 0\ \cdots\ \beta_{\rho+i,\,\rho+i}\ \cdots\ 0\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\\
0\quad 0\ \cdots\cdots\cdots\ 0 & 0\ \cdots\cdots\cdots\ 1
\end{array}\right|\equiv 1 \pmod{p^{\kappa}},\qquad \delta\equiv 1 \pmod{p^{\kappa}},$$

---

*Cf. Clebsch u. Gordan, Abel'sche Funktionen, p. 300.

provided that
$$\begin{vmatrix} \beta_{ii}, & \beta_{i,\,\rho+i} \\ \beta_{\rho+i,\,i}, & \beta_{\rho+i,\,\rho+i} \end{vmatrix} \equiv 1 \pmod{p^\kappa}.$$

We shall call the transformation in which β_{ij} and δ have these values *the transformation* A_i. Similarly, *the transformation* B_{ij} shall be the transformation in which δ and the β's have the following values:

$$|\beta| \equiv \begin{array}{|l|l|l}
1 \quad 0 \ldots\ldots 0 \ldots\ldots\ldots\ldots 0 \ldots\ldots\ldots 0 & 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & \\
0 \quad 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\ldots\ldots \ddots \beta_{ii} \ldots\ldots 0 \ldots \beta \ldots\ldots 0 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\ldots\ldots 0 \,..\, 1 \ldots\ldots\ldots 0 \ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\ldots\ldots\ldots\ldots\ldots \ddots 1 \ldots\ldots 0 \ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\ldots\ldots \beta_{ji} \ldots 0 \ldots 0 \ldots \ddots \beta_{jj} \ldots\ldots 0 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ddots 1 \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
0 \quad 0 \ldots 0 \ldots\ldots 0 \ldots\ldots 0 \,..\, 0 \ldots \ddots 1 & 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & \\
\hline
0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & 1 \quad 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & \equiv 1 \pmod{p^\kappa}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & 0 \quad 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \quad \ddots \beta_{\rho+i,\,\rho+i}\beta_{\rho+i,\,\rho+j} \ldots\ldots & \delta \equiv 1 \pmod{p^\kappa} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \qquad \vdots \qquad\qquad \vdots & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots \beta_{\rho+j,\,\rho+i}\beta_{\rho+j,\,\rho+j} \ldots\ldots & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 & 0 \quad 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 1 &
\end{array}$$

provided that
$$\begin{vmatrix} \beta_{ii}, & \beta_{ij} \\ \beta_{ji}, & \beta_{jj} \end{vmatrix} \cdot \begin{vmatrix} \beta_{\rho+i,\,\rho+i}, & \beta_{\rho+i,\,\rho+j} \\ \beta_{\rho+j,\,\rho+i}, & \beta_{\rho+j,\,\rho+j} \end{vmatrix} \equiv 1 \pmod{p^\kappa}.$$

Therefore, any set of values satisfying the condition $\begin{vmatrix} \beta_{ii}, & \beta_{ij} \\ \beta_{ji}, & \beta_{jj} \end{vmatrix} \not\equiv 0 \pmod{p}$ is admissible.

58. In case m_i and $m_{\rho+i}$ are not both $\equiv 0 \pmod{p}$, it is always possible (remembering that we have already made every $m < p$), by the transformation A_i to make $m_i' \equiv 1$, $m_{\rho+i}' \equiv 0 \pmod{p^\kappa}$. The m's have now been reduced to such values that
$$m_{\rho+i}' \equiv 0 \pmod{p^\kappa}, \; i = 1, 2, \ldots . \rho,$$
and at least one m_i' is $\not\equiv 0 \pmod{p}$ since $A = 1$.

If m'_i and m'_j, $(j > i)$ are not both $\equiv 0 \pmod{p}$, it is always possible by the transformation B_{ij}, to make

$$\begin{aligned} m''_i &\equiv 1 \pmod{p^\kappa}, \\ m''_j &\equiv 0 \;(\;\;\text{"}\;\;). \end{aligned}$$

This transformation leaves all other m's unaltered. By successive applications of B_{ij}, the m's are reduced to

$$m_1 \equiv 1 \pmod{p^\kappa},\ m_j \equiv 0 \pmod{p^\kappa}, j = 2, 3, \ldots . 2\rho,$$

i. e. all the sets of values of m_i for which $A = 1$ can be reduced to the above set, and there is hence but a single group when $A = 1$.

Groups, Type $(\varkappa)(11 \ldots . 1),\ p > 2$.

$$\begin{array}{ll|c|c|l} A & = & 1 & p & \\ a^{p^\kappa} & = & 1 & 1 & \\ b_1^p & = & a & 1 & \\ b_j^p & = & 1 & 1 & j = 2, 3, \ldots . 2\rho. \end{array}$$

In both groups,

$$\begin{aligned} b_j b_i &= a^{p^{\kappa-1}} b_i b_j, \text{ if } i = j - \rho \\ &= a^{-p^{\kappa-1}} b_i b_j, \text{ if } i = j + \rho, \\ &= b_i b_j \text{ in all other cases,} \\ &\qquad i, j = 1, 2, \ldots . 2\rho, \text{ independently,} \\ a b_i &= b_i a, \quad i = 1, 2, \ldots . 2\rho. \end{aligned}$$

59. *Case* $p = 2$.

Formulæ of Transformation:

$$m'_i \equiv 2\alpha_i + \sum_{j=l+1}^{s} \sum_{l=1}^{s-1} \beta_{il}\beta_{ij} n_{lj} + \sum_{j=1}^{s} \beta_{ij} m_j \pmod{2^\kappa},$$

$$n'_{ij} \equiv \sum_{\kappa=1}^{s} \sum_{l=1}^{s} \beta_{il}\beta_{j\kappa} n_{l\kappa} \pmod{2^\kappa},\ i = 1, 2, \ldots . s - 1,\ j = i + 1, \ldots . s.$$

Since n_{lj} is divisible by $2^{\kappa-1}$ (No. 53), it follows that, when $\varkappa > 1$, the second term in the expression above for m_i is a multiple of 2 and can therefore be taken together with the term $2\alpha_i$, in which α_i is a perfectly arbitrary quantity. In this way the formulæ of transformation become precisely those of the case $p > 2$. It is therefore not necessary to consider separately the case $p = 2$ unless $\varkappa = 1$. *The groups of type* $(\varkappa)(11 \ldots . 1)$ *are those of No.* 58, *irrespective of the value of* p.

60. We consider, then,

Type (1)(11 . . . . 1), $p = 2$.

Formulæ of Transformation:

$$m_i' \equiv \sum_{j=l+1}^{s} \sum_{l=1}^{s-1} \beta_{il}\beta_{ij} n_{lj} + \sum_{j=1}^{s} \beta_{ij} m_j \pmod{2}, \quad i = 1, 2, \ldots . s,$$

$$n_{ij}' \equiv \sum_{\kappa=1}^{s} \sum_{l=1}^{s} \beta_{il}\beta_{j\kappa} n_{l\kappa} \pmod{2}, \quad i = 1, 2, \ldots . s-1, \quad j = i+1, \ldots . s.$$

As in No. 56, we apply first a transformation making

$$n_{i,\,\rho+i} \equiv n_{\rho+i,\,i} \equiv 1 \pmod{2}, \quad i = 1, 2, \ldots . \rho,$$
$$n_{ij} \equiv 0 \pmod{2} \text{ for all other values of } i \text{ and } j.$$

The transformation A_i has the following results:

$$m_i' \equiv \beta_{ii}\beta_{i,\,\rho+i} + \beta_{ii} m_i + \beta_{i,\,\rho+i} m_{\rho+i} \pmod{2},$$
$$m_{\rho+i}' \equiv \beta_{\rho+i,\,i}\beta_{\rho+i,\,\rho+i} + \beta_{\rho+i,\,i} m_i + \beta_{\rho+i,\,\rho+i} m_{\rho+i} \pmod{2},$$
$$m_j' \equiv m_j \pmod{2}, \text{ if } j \ddagger i \text{ or } \rho + i.$$

By means of this transformation m_i' and $m_{\rho+i}'$ can both be made $\equiv 0 \pmod{2}$ except when m_i and $m_{\rho+i}$ are both congruent unity (mod 2), when necessarily also

$$m_i' \equiv m_{\rho+i}' \equiv 1 \pmod{2}.$$

The transformation B_{ij} has the following results:

$$m_i' \equiv \beta_{ii} m_i + \beta_{ij} m_j \pmod{2},$$
$$m_j' \equiv \beta_{ji} m_i + \beta_{jj} m_j \pmod{2},$$
$$m_{\rho+i}' \equiv \beta_{\rho+i,\,\rho+i},\, m_{\rho+i} + \beta_{\rho+i,\,\rho+j} m_{\rho+j} \pmod{2},$$
$$m_{\rho+j}' \equiv \beta_{\rho+j,\,\rho+i},\, m_{\rho+i} + \beta_{\rho+j,\,\rho+j} m_{\rho+j} \pmod{2},$$
$$m_\kappa' \equiv m_\kappa \pmod{2} \text{ for all other values of } \kappa.$$

Provided at least one of the numbers m_i, m_j, is $\equiv 1 \pmod{2}$, we can, by this transformation, make

$$m_i' \equiv 1 \pmod{2},$$
$$m_j' \equiv 0 \;(\;\text{``}\;).$$

By successive applications of the transformations A_i and B_{ij}, any possible set of m's can be reduced to one of the two following:

$$\begin{array}{cccccccc} m_1, & m_2, & \ldots . & m_\rho, & m_{\rho+1}, & m_{\rho+2}, & \ldots . & m_{2\rho}, \\ 1, & 0, & \ldots . & 0, & 1, & 0, & \ldots . & 0, \\ 0, & 0, & \ldots . & 0, & 0, & 0, & \ldots . & 0. \end{array}$$

These two sets of values *may* be reducible into each other. According as they are or are not so reducible, the type has one or two groups. I have not succeeded either in effecting the reduction or in proving its impossibility; nor have I been able to find an invariant by whose different values the groups of the type could be distinguished.

There are, then, *at most* two groups of the type (1)(11 . . . . 1), $p = 2$; they are generated by elements satisfying the following relations:

$$\begin{array}{ll|c|c|l}
a^2 & = & 1 & 1 & \\
b_1^2 & = & a & 1 & \\
b_{\rho+1}^2 & = & a & 1 & \\
b_i^2 & = & 1 & 1 & i = 2, 3, \ldots\ldots \rho, \ \rho + 2, \ldots\ldots 2\rho.
\end{array}$$

In both groups

$$\begin{aligned}
ab_i &= b_i a, \quad i = 1, 2, \ldots\ldots 2\rho, \\
b_j b_i &= a b_i b_j, \text{ if } i = j \pm \rho, \\
&= b_i b_j \text{ in all other cases.}
\end{aligned}$$

61. *Type* (1)(1)(11 . . . . 1), $s = 2\rho$ units in the last parenthesis.

Every group of this type is generated by elements

$$a, \ b, \ c_i, \ (i = 1, 2, \ldots\ldots 2\rho),$$

satisfying the relations:

$$\begin{aligned}
& a^p = 1, \\
& b^p = a^m, \\
& \left.\begin{aligned} c_i^p &= a^{n_i} b^f, \\ c_i b &= a^{q_i} b c_i, \end{aligned}\right\} i = 1, 2, \ldots\ldots 2\rho, \\
& c_j c_i = a^{t_{ij}} b^{h_{ij}} c_i c_j, \quad i, j = 1, 2, \ldots\ldots 2\rho, \text{ independently}, \\
& ab = ba, \\
& ac_i = c_i a, \quad i = 1, 2, \ldots\ldots 2\rho.
\end{aligned}$$

If in these relations we consider $a = 1$, we have (No. 12) the relations satisfied by the generating elements of a group of type (1)(11 . . . . 1). But we have just considered this type and have seen that the following restrictions may be imposed on the exponents in the generating relations without thereby excluding any group of the type:

$$\begin{aligned}
m_i &\equiv \quad 0 \pmod{p}, \text{ unless } i = 1 \text{ or } \rho + 1, \\
n_{ij} &\equiv \begin{cases} 1 \pmod{p}, \text{ if } i = i + \rho, \\ -1 \pmod{p}, \text{ if } j = i - \rho, \\ 0 \pmod{p} \text{ in all other cases.} \end{cases}
\end{aligned}$$

We may, therefore, without excluding any groups, impose the same restrictions on the corresponding exponents in the present type, viz:

$$f_i \equiv 0 \pmod{p}, \text{ unless } i = 1 \text{ or } \rho + 1,$$

$$h_{ij} \equiv \begin{cases} 1 \pmod{p}, \text{ if } j = i + \rho, \\ -1 \pmod{p}, \text{ if } j = i - \rho, \\ 0 \pmod{p} \text{ in all other cases.} \end{cases}$$

By the usual methods it is seen that the necessary and sufficient condition that no element other than a and its powers be commutative with every element of the group, is that *at least one of the integers* q_i *be not congruent zero* (*mod* p).

62. Most of the relations resulting from transforming the given relations by each of the generating elements are products and powers of the given relations. In the following case, however (among others), the resulting relations are not so expressible.

Transforming the relation

$$c_j c_i = a^{t_{ij}} b^{h_{ij}} c_i c_j,$$

by c^κ, the relation results $\quad a^{h_{ij} q_\kappa + h_{j\kappa} q_i + h_{\kappa i} q_j} = 1,$

whence (note No. 20),

$$h_{ij} q_\kappa + h_{j\kappa} q_i + h_{\kappa i} q_j \equiv 0 \pmod{p}, \; i, j, \varkappa = 1, 2, \ldots . \; 2\rho, \text{ independently.}$$

If $\rho = 1$, the indices i, j, $\varkappa$ cannot all be distinct, but at least two must be equal, say $j = \varkappa$, and the congruence above becomes

$$h_{ij} q_j + h_{jj} q_i + h_{ji} q_j \equiv 0 \pmod{p}.$$

This is an identity, since $h_{ij} \equiv - h_{ji}$, $h_{jj} \equiv 0 \pmod{p}$.

But if $\rho > 1$, we can choose i arbitrarily, and $j \neq i \pm \rho$, $\varkappa = j \pm \rho$, when the congruence becomes

$$h_{ij} q_{j \pm \rho} + h_{j, j \pm \rho} q_i + h_{j \pm \rho, i} q_j \equiv 0 \pmod{p}, \; i = 1, 2, \ldots . \; 2\rho.$$

But, since $j \neq i \pm \rho$,

$$h_{ij} \equiv 0, \; h_{j \pm \rho, i} \equiv 0, \; h_{j, j \pm \rho} \not\equiv 0 \pmod{p}.$$

Substituting these values we have

$$h_{j, j \pm \rho} q_i \equiv 0 \pmod{p}, \; i = 1, 2, \ldots . \; 2\rho.$$

Whence $\quad q_i \equiv 0 \pmod{p}, \; i = 1, 2, \ldots . \; 2\rho.$

This is a necessary consequence of the generating relations given. But we have seen that, in order that the elements satisfying the relations given shall generate a group of the type under consideration, it is necessary that at least one of the quantities q_i be *not* congruent zero, (mod p). *There are, therefore, when* $\rho > 1$, *no groups of the type* $(1)(1)(11 \ldots . 1)$. The case $\rho = 1$, type $(1)(1)(11)$, has already been considered.

CLARK UNIVERSITY, WORCESTER, MASS., *August* 12, 1892.